

VERBATIM ¹RECORD OF TRIAL ²

(and accompanying papers)

of

MANNING, Bradley E.

(Name: Last, First, Middle Initial)

Headquarters and
Headquarters Company,
United States Army Garrison

(Unit/Command Name)

[REDACTED]

(Social Security Number)

U.S. Army

(Branch of Service)

PFC/E-3

(Rank)

Fort Myer, VA 22211

(Station or Ship)

By

GENERALCOURT-MARTIAL

Convened by

Commander

(Title of Convening Authority)

UNITED STATES ARMY MILITARY DISTRICT OF WASHINGTON

(Unit/Command of Convening Authority)

Tried at

Fort Meade, MD

(Place or Places of Trial)

on

see below

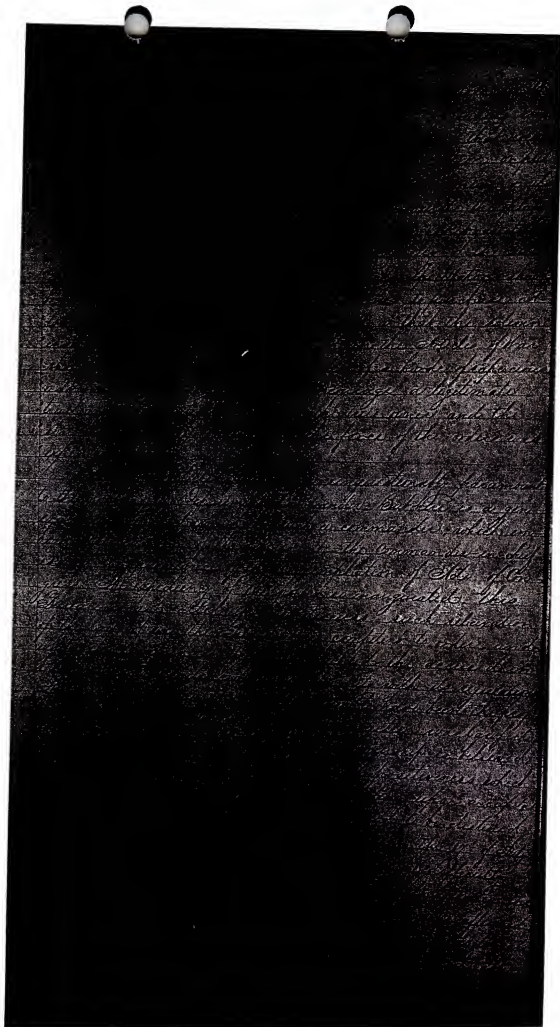
(Date or Dates of Trial)

Date or Dates of Trial:

23 February 2012, 15-16 March 2012, 24-26 April 2012, 6-8 June 2012, 25 June 2012, 16-19 July 2012, 28-30 August 2012, 2 October 2012, 12 October 2012, 17-18 October 2012, 7-8 November 2012, 27 November - 2 December 2012, 5-7 December 2012, 10-11 December 2012, 8-9 January 2013, 16 January 2013, 26 February - 1 March 2013, 8 March 2013, 10 April 2013, 7-8 May 2013, 21 May 2013, 3-5 June 2013, 10-12 June 2013, 17-18 June 2013, 25-28 June 2013, 1-2 July 2013, 8-10 July 2013, 15 July 2013, 18-19 July 2013, 25-26 July 2013, 28 July - 2 August 2013, 5-9 August 2013, 12-14 August 2013, 16 August 2013, and 19-21 August 2013.

¹ Insert "verbatim" or "summarized" as appropriate. (This form will be used by the Army and Navy for verbatim records of trial only.)

² See inside back cover for instructions as to preparation and arrangement.



)))))))))

 γ_0

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

**Government Targeted Brief
On Receipt of Intelligence
as a Requirement of
Aiding the Enemy
Enclosure 4**

29 March 2013

Encl 4 to
APPELLATE EXHIBIT 510
PAGE REFERENCED: _____
PAGE _____ OF _____ PAGES

MILITARY LAW REVIEW Vol. 30

Articles

NUCLEAR WEAPONS AS A LAWFUL MEANS

Captain Fred Bright, Jr.

TREASONS AND AIDING THE ENEMY

Captain Jabez W. Loane, IV

THE SIGNIFICANCE OF THE JENCKS ACT IN MILITARY LAW

Major Luther C. West

Comments

ASSASSINATION IN WAR TIME

LEGAL SUPPORT REQUIREMENTS FOR CIVIL AFFAIRS OPERATIONS IN COUNTERINSURGENCY

SOME OBSERVATIONS ON LESSER INCLUDED OFFENSES

HEADQUARTERS, DEPARTMENT OF THE ARMY

OCTOBER 1965

TREASON AND AIDING THE ENEMY*

BY CAPTAIN JABEZ W. LOANE, IV**

I. INTRODUCTION

It has been said that no crime is greater;¹ it has been termed “. . . the most serious offense that may be committed against the United States;”² it has been classified as “the highest of all crimes.”³ Chief Justice Marshall once commented: “As there is no crime which can more excite and agitate the passions of men, no charge demands more from the tribunal before which it is made a deliberate and temperate inquiry.”⁴ All of these quotations refer to the same offense—the crime of treason.

It is a crime which, in many ways, is set apart from all others. It is the only crime specifically denounced by the Constitution of the United States.⁵ It is the only federal crime upon which conviction must be predicated on the testimony of two eye-witnesses to the overt act of the offense.⁶ It may only be committed in time of war or quasi war since it must be predicated either in levying war against the United States or in aiding an “enemy.” It is the only crime which, if successfully committed, may cease to be a crime. As Sir John Harrington noted:

Treason doth never prosper; what's the reason? Why, if it prosper, none dare call it treason.⁷

* This article was adapted from a thesis presented to The Judge Advocate General's School, U.S. Army, Charlottesville, Virginia, while the author was a member of the Thirteenth Career Course. The opinions and conclusions presented herein are those of the author and do not necessarily represent the views of The Judge Advocate General's School or any other governmental agency.

** JAGC, U. S. Army; Office of the Staff Judge Advocate, Hq, U. S. Army, Europe; A.B., 1953, Duke University; LL.B., 1956, University of Maryland; Member of the Bars of the State of Maryland, the United States Supreme Court, and the United States Court of Military Appeals.

¹ Hanauer v. Doane, 79 U.S. (12 Wall.) 342, 347 (1870).

² Stephen v. United States, 133 F.2d 87, 90 (6th Cir.), cert. denied, 318 U.S. 781 (1943).

³ Charge to Grand Jury, 30 Fed. Cas. 1024, 1025 (No. 18269) (C.C.D. Mass. 1851).

⁴ Marshall, C. J., in *Ex Parte Bollman*, 8 U.S. (4 Cranch) 75, 125 (1807).

⁵ U. S. CONST. art. III, § 3.

⁶ *Ibid.* This assumes, of course, a plea other than guilty. However, it should be noted that some states require two witnesses to any crime punishable by death. See *State v. Chin Lung*, 106 Conn. 701, 139 A. 91 (1929).

⁷ FAMILIAR QUOTATIONS 29 (12th ed. Morley Ed., 1951).

30 MILITARY LAW REVIEW

Throughout the ages the motivations for treason have been as numerous as the crimes themselves. Some have committed treason for money, some for pride, power, or prestige, some for more elusive ideological goals. In medieval England, where our exploration of the law begins, the treason cases generally dealt with machinations against the monarch or in plotting to alter the succession to the throne. In the days of Elizabeth I, the cases developed a religious, flavor. In later years, the factors have included financial gain or political conviction. Today the suggestion has been advanced that the modern scientist, because of the universality of his technical knowledge, feels himself under a lesser duty to obey national loyalty.⁸

The annals of treason have tainted the rich and poor alike; the powerful as well as the common citizen. Through its history have passed such notable figures as Thomas Becket, Sir Walter Raleigh, Anne Boleyn, Sir Thomas More, Benedict Arnold, and Jefferson Davis; it has included such strange personalities as Guy Fawkes, John Brown, William Joyce and Ezra Pound. And it has encompassed the unnumbered hundreds who passed through the musty volumes of the State Trials⁹ on their way to the "usual punishment" and oblivion.

It is not the purpose of this article to examine these individuals in depth or the details of the "offenses" which brought them to trial. Rather it is intended to explore the historical development of the civil offense of treason and the parallel military offense of aiding the enemy; to compare the two; and to consider the defenses to the respective offenses. For indeed, until comparatively recently, the mere fact of the indictment was tantamount to conviction and little other than outright denial was available to an unfortunate defendant.

It is hoped that this article will help to solve some of the many problems which may easily be conceived. When, for example, may an American sufficiently shake off his citizenship that he can aid America's enemy and avoid a treason charge? Is physical opposition to the enforcement of the laws of the United States by its officers treason? If so, were the students at the University of Mississippi guilty of treason by participating in the 1962 riots? Can a citizen "adhere" to an enemy without "aiding"

⁸ WEST, *THE NEW MEANING OF TREASON* (1964).

⁹ Howell, *A Complete Collection of State Trials and Proceedings for High Treason and Other Crimes and Misdemeanors from the Earliest Period to the Present Time* (1816) [hereafter cited as *How. St. Tr.*]

him, and, conversely can he "aid" the enemy without "adherence"? Is a soldier who conducts propaganda lectures for the enemy in a POW camp guilty of giving them "aid"? If so would it make any difference if none of the other prisoners were affected? What is the status of the alien who resides in this country? Is this status affected if he is a citizen of an "enemy" country? The situations may be ingenuously contrived. The courts must wrestle for the answers.

II. THE HISTORY OF TREASON

A. *THE ENGLISH BACKGROUND*

There is no better introduction to the law of treason in the United States than a short review of the English law, since the present American law is directly traceable to a statute published by Edward III in 1350.¹⁰ During the early fourteenth century England was in a state of flux. These were days of constant civil war attended by one parliamentary crisis after another. When one faction gained power it frequently subjected the nobles and landowners of the other to the harassment of trial for treason based solely on political or quasi-political considerations. As no legal definition of treason existed, no one could foretell what action or word might be interpreted as committing the offense." An additional troublesome area concerned the fact that lands and possessions of anyone convicted of treason were subject to attainder or forfeiture.¹²

There was, understandably, increasing agitation that the offense be more rigidly defined. To the barons and large landowners this argument was quite persuasive in view of the forfeiture provisions.¹³ In addition, the definition was of importance in restraining the power of the crown to suppress any subject by arbitrary construction of the law.

¹⁰ Statute of Purveyors, 1350, 25 Edw. 3, Stat. 5, c. 2.

¹¹ For the proposition that it was still difficult to tell after the statute see *Carpenters Case*, 11 Henry VI (1434), digested in BUND, *A SELECTION OF CASES FROM THE STATE TRIALS* 29 (1st ed. 1879), where a convicted wife murderer was also adjudged a traitor in order that he might receive the greater punishment as an "example." The same fate befell the convicted murderer of the Duke of Gloucester, *Proceedings Against John Hall*, 1 How. St. Tr. 162 (1399).

¹² Clarke, *Forfeitures and Treason in 1388*, 14 ROYAL HIST. SOC. TRANS. 4th 65 (1931).

¹³ Perhaps because of continuing pressure Edward III further modified the attainder provisions in 1360 to provide no forfeiture for persons not attained in their lifetime. Statute of Westminster, 1360, 34 Edw. 3, c. 12.

30 MILITARY LAW REVIEW

Eventually the King yielded to the pressures. There resulted the famous statute of 25 Edward III which defined the offense as being committed:

When a man doth compass or imagine the death of our lord the King, or of our Lady his Queen, or of their eldest son and heir; or if a man doth violate the King's companion, or the King's eldest daughter unmarried, or the wife [of] the King's eldest son and heir; or if a man do levy war against our lord the King in his realm, or be adherent to the King's enemies in his realm, giving them aid and comfort in the realm or elsewhere, and thereof be provably attainted of open deed by the people in their condition."

The statute goes on to define five other acts which may constitute treason (e.g., counterfeiting, assaulting certain of the King's officers), and concludes with what, for those days, must have been a novel proposition, that no other act would constitute treason unless made so by act of King and Parliament.¹⁵ Shorn of the language concerning the monarch and those portions intended to purify the succession, the statute can be fairly said to state the American definition today.

That Edward III defined the offense was laudable. Yet many of the pre-statutory problems remained. One reason for this was that the courts possessed the power of interpreting the statute and could thus put whatever meaning they chose on such vague phrases as "compass or imagine" and "giving them aid or comfort."¹⁶ In 1668, for example, members of a riotous group engaged in pulling down "bawdy houses" who failed to obey a Constable's order to desist were convicted of treason, the court holding that this constituted "levying war" against the King.¹⁷ An additional problem was the personality of the monarch. Under the "strong" monarchs the offense tended to have much wider definition. During the reign of Henry VIII, the crime is considered to have had its widest interpretation. As a matter of fact, Henry VIII extended treason to cover such situations as wishing harm to the King or calling him a tyrant.¹⁸ However, a reading of the cases in the days of Elizabeth I would tempt a contrary conclusion as

¹⁵ Statute of Purveyors, 1350, 25 Edw. 3, Stat. 5, c. 2.

¹⁶ *Ibid.*

¹⁷ For an extreme position see the Trial of Algernon Sidney, 9 How. St. Tr. 818 (1683). Sidney was convicted solely on evidence of possession of unpublished manuscripts. It is difficult to see how this "compassed the death" of the King.

¹⁸ Trial of Peter Messenger, 6 How. St. Tr. 879 (1668).

¹⁹ For a good discussion of treason during the reign of Henry VIII, see Thornly, *The Treason Legislation of Henry VIII*, 11 ROYAL HIST. SOC. TRANS. 3d 87 (1917).

to treason's golden age. It is reported that after the Northern Rebellion of 1569, Elizabeth had some 1,200 peasants executed as traitors, many on mere suspicion, and without the benefit of a trial.¹⁹

Thus, notwithstanding the apparent clarity of the Statute of Edward III, the law of treason continued to be drawn by a wavering hand. Justice was dependent upon the whim of the King or the policy of the judge. The rights of an accused seemed to have returned to the early days of anarchy. It was not until 1695 that the substantive law was backed up by procedural guarantees. This was the date of the enactment of the so-called "Treason Trials Act" which was to play an important part in the growth of the American law.²⁰ Considering the harsh justice meted out by the Tudor courts, this statute is remarkable in expanding the rights of an accused. First, it provided that the accused was entitled to a copy of the indictment five days prior to trial (although not the names of the witnesses).²¹ Secondly, he was entitled to be represented by counsel.²² Commoners were granted a jury trial consisting of 12 freeholders who were required to vote unanimously in order to convict.²³ In addition, a statute of limitations was established as three years.²⁴ But finally, and most important, it spelled out another rule which has come to be regarded as fundamental. In the absence of a confession a conviction could only be had by the testimony of at least two witnesses to the overt act of treason.²⁵ And it was carefully postulated that if two or more treasons were charged in the indictment it was necessary that there be two witnesses to each separate act.²⁶

In concluding that the English law has carried over almost verbatim to the American it may be well to touch tangentially on the one phase which, fortunately, has not. That was the so-called "usual sentence" which was meted out to the convicted traitor.

¹⁹ BUND, *op. cit. supra* note 1, at 219.

²⁰ Statute of Westminster, 1695, 7 & 8 William 3, c. 3.

²¹ *Ibid.*

²² Prior to this act counsel was forbidden. The accused could merely represent himself and this was largely at the mercy of the attorney for the crown. For a notorious example see the prosecution by Edward Coke in the Trial of Sir Walter Raleigh, 2 How. St. Tr. 1 (1603).

²³ Also to acquit.

²⁴ Probably motivated by the case of the trial of Colonel Algernon Sidney, 9 How. St. Tr. 818 (1683), who complained that the evidence against him may have been 20 to 30 years old. He was executed.

²⁵ Statute of Westminster, 1795, 7 & 8 William 3, c. 3.

²⁶ *Ibid.*

30 MILITARY LAW REVIEW

An illustration of the hideous barbarism can be vividly demonstrated by the sentence given Thomas Howard, Duke of Norfolk, in 1571:

Wherefore thou shalt be had from hence to the Tower of London, from thence thou shalt be drawn through the midst of the streets of London to Tyburn, the place of execution; there thou shalt be hanged, and being alive thou shalt be cut down quick, thy bowels shall be taken forth of thy body, and burnt before thy face, thy head shall be smitten off, thy body shall be divided into four parts or quarters; thy head and thy quarters to be set up where it shall please the queen's majesty to appear; and the Lord shall have mercy upon thou."

For commoners the sentence often included the removal of privy parts prior to disemboweling.²⁸ The Duke was lucky. As with most nobles, his sentence was commuted to simple beheading. Others were not so fortunate. It is surprising that this sentence continued to be given in the Nineteenth Century,²⁹ and is reported to have been pronounced (although not carried out) as late as 1867.³⁰ By this time the minimum penalty in the United States was five years imprisonment and a \$10,000 fine.

It does not appear that any consideration was ever given to adopting the "usual sentence" in the United States.

B. THE CONSTITUTIONAL VIEW OF TREASON

Prior to the Revolution there existed in the colonies a variety of statutes, decrees, and royal grants which recognized the existence of the crime of treason.³¹ Reported law prior to the formation of the United States is rare. The only available extensive record of trial is the case of Colonel Nicholas Bayard who was tried in the province of New York for high treason in 1702.³² Bayard was tried under a New York statute which provided that it was treason to disturb "by force of arms, or other ways, . . . the peace, good, and quiet of this their majesties' government, as it is now established . . ." ³³ Bayard's offense appears to have been that of circulating a petition deemed critical of the provincial government. Notwithstanding an opinion from the attorney gen-

²⁸ Trial of Thomas Howard, Duke of Norfolk, 1 How. St. Tr. 957, 1031 (1571).

²⁹ See, e.g., Trial of William Parry, 1 How. St. Tr. 1095, 1111 (1584).

³⁰ See, e.g., Trial of E. M. Despard, 28 How. St. Tr. 346, 527 (1803).

³¹ WEYL, TREASON 7 (1950).

³² For a collection of the various Colonial laws see, Hurst, *Treason in the United States*, 58 HARV. L. REV. 226 (1944).

³³ Trial of Colonel Nicholas Bayard, 14 How. St. Tr. 471 (1702).

³⁴ Id. at 473.

eral that this did not amount to treason, Bayard was tried, convicted and given the "usual sentence." Fortunately, there was a change of Governors and the conviction was reversed. The point to be drawn from the case is that, notwithstanding the fact that the trial was predicated on a New York law bearing no significance to the Statute of Edward III, the legal arguments in the case all revolved on that English statute.³⁴ While the language may have been changed to fit the immediate needs of the emerging colonies, the image of treason continued in its English form.

During the Revolutionary War, treason underwent a change. The emerging states began to enact laws making it treason to adhere to George III or his forces. These varied in language but all followed the Statute of Edward III, either by similar language or by express reference.³⁵

When the framers met to establish a Constitution a definition of treason was indeed important in their minds. But there must have been much soul searching. In the first place, the framers had just finished committing treason themselves, at least so far as the English were concerned. On the other hand, they had vivid recollections as to the danger of internal treason. The plot of Benedict Arnold and the activities of the loyalist Tories had almost wrecked the fledgling nation they were striving to promote.

How should treason be defined—by the Constitution itself or the Congress? The Pinckney Report,³⁶ provided for it to be done by Congress.³⁷ So, apparently, did the New Jersey plan.³⁸ But thereafter, the framers had second thoughts, It may be surmised that they, like the barons of 1350, felt the offense of treason needed a rigid definition, free from the whims of a subsequent legislative body. The Committee on Detail rejected both proposed versions and substituted its own:

Treason against the United States shall consist only in levying war against the United States, or any of them; and in adhering to the enemies of the United States, or any of them. The Legislature of the United States shall have the power to declare the punishment of treason.

³⁴ *Id.*

³⁵ Hurst, *supra* note 31, at 226, 256-57.

³⁶ Charles C. Pinckney, delegate from South Carolina.

³⁷ 2 FARRAND, RECORDS OF THE FEDERAL CONVENTION OF 1787, at 136 (1937).

³⁸ 3 FARRAND, *op. cit.* *supra* note 37, at 614.

30 MILITARY LAW REVIEW

No person shall be convicted of treason, unless on the testimony of two witnesses. No attainder of treason shall work corruption of blood nor forfeiture, except during the life of the person attained."

The Legislature was to retain the power to fix the punishment but not to define the crime. Understandably the debates on the subject proved lively.⁴⁰ James Madison opened the issue by contending that the proposed definition did not go as far as the Statute of Edward III and that more latitude ought to be left to the states. Madison's thinking on the latter was doubtlessly influenced by the Virginia experience of Bacon's rebellion which was directly solely against the local government. The thrust of his contention involved a proposal to insert the phrase "giving them aid and comfort." Interestingly enough the delegates themselves split on the effect of such insertion. Some thought the words would extend the definition of treason; some, with whom the author concurs, found them restrictive; some were satisfied that they were mere words of explanation. In the end, the motion to insert the words carried.⁴¹ A sharp dispute next developed as to whether the states would still retain the right to enact laws for treason against the state. Madison wanted them to retain this power. By a 6 to 5 vote, the delegates voted to limit the constitutional provision to treason "against the United States."⁴² At Dr. Franklin's urging the language requiring two witnesses to the same overt act, one of the guarantees of the Treason Trials Act, was included by an 8 to 3 majority.⁴³ Final debate centered about whether to permit confession in open court alone to be sufficient for conviction. The delegates agreed that such would suffice, although some considered the language superfluous. It was inserted.

In conclusion, then, the delegates had hammered out what would thereafter constitute treason against the United States. The end product, which was included in the new constitution, provided:

Treason against the United States, shall consist only in levying war against them or in adhering to their enemies, giving them Aid and Comfort. No person shall be convicted of Treason unless on the Testi-

⁴⁰ 2 *id.* at 182.

⁴¹ See *id.* at 345-50; MADISON, THE DEBATES IN THE FEDERAL CONVENTION OF 1787 WHICH FRAMED THE CONSTITUTION OF THE UNITED STATES OF AMERICA, 430-34 (Int'l ed., Hunte Scott ed. 1920).

⁴² 2 FARRAND, *op. cit.* supra note 37, at 345-46.

⁴³ *Id.* at 349.

⁴⁴ *Id.* at 348.

mony of two Witnesses to the same overt Act, or on Confession in open Court."

A reading of the provision discloses a final sentence as to which no discussion is found in the available records.

The Congress shall have the Power to declare the Punishment of Treason, but no Attainder of Treason shall work Corruption of Blood, or Forfeiture except during the Life of the Person attained."

One problem alone remained for discussion—should the President have the power to pardon convicted traitors. Virginia supported an exception to the executive pardoning power of the President in cases of treason. Reasoned Mr. Randolph: "The President himself may be guilty."⁴⁶ But the counter-argument ran that pardon is a necessary power and that should the President himself commit the offense he could always be impeached.⁴⁷ On the vote only Virginia and Georgia supported the motion.⁴⁸

C. THE DEVELOPMENT OF THE FEDERAL LAW

Having been given the authority Congress proceeded quickly to implement it. The Act of April 30, 1790, after carefully reciting the substantive guidelines specified by the Constitution, set the punishment for treason as death.⁴⁹ In establishing procedural safeguards, Congress included its up-to-date version of the Treason Trials Act and specifically permitted an accused qualified counsel and the authority to subpoena defense witnesses.⁵⁰ It also required that the accused be furnished a copy of the indictment and the names and addresses of prospective jurors and witnesses at least three days prior to trial.⁵¹ The act entitled the defendant to challenge up to 35 jurors peremptorily, and, concerned about a failure to plead, provided that if the accused either stood mute, or refused to plead, the court would proceed to try the case as on a plea of "Not Guilty."⁵²

It was under this statute that the courts had their first taste of "American Plan" treason. During the administration of Wash-

⁴⁶ U.S. CONST. art. III §, 3.

⁴⁷ It was apparently lifted from an earlier draft and inserted by the Committee of Style. See 2 FARRAND, *op. cit. supra* note 37, at 601.

⁴⁸ *Id.* at 626.

⁴⁹ The counterargument was made by Mr. Wilson of Pa., who had recently represented four defendants tried for treason in Pa. courts.

⁵⁰ 2 FARRAND, *op. cit. supra* note 37, at 627.

⁵¹ Act of April 30, 1790, 1 Stat. 112.

⁵² 1 Stat. 112, at 118.

⁵³ *Ibid.*

⁵⁴ 1 Stat. 112, at 119.

ington and Adams the new treason law was applied twice. One instance arose out of the "Whiskey Rebellion" of 1794, the second out of "Fries' Rebellion" in 1798. Both involved a judicial interpretation of what constituted "levying war." Shortly thereafter came the machinations of Aaron Burr and the subsequent trials of the ex-Vice President and others for treason. Burr's case involved the technical legal problems involved in proving the "overt act."

The states proceeded to enact their own laws of treason as they were permitted to do under the Constitution. But the applications of such statutes has been minimal. Only two cases of completed prosecutions by a state have been uncovered: one involving Thomas Dorr by Rhode Island, and one involving John Brown by Virginia.⁵³ The former was sentenced to prison for life, the latter was executed. John Brown and five of his band of raiders hold the distinction of being the only men executed for treason by either state or federal authorities in the United States.⁵⁴

As the nation grew the number of prosecutions for treason continued to be few. True each war brought its share of recalcitrants. The War of 1812 had its Federalists and the Mexican War its Whigs.⁵⁵ But military opposition to the Government by its citizens did not occur again until 1857. This was the full scale disobedience by the Mormons in Utah that eventually led to military opposition to the Army units sent to restore order. With uncharacteristic fury, President Buchanan issued a proclamation to the Mormons:

Fellow citizens of Utah! this is rebellion against the government to which you owe allegiance. It is levying war against the United States, and involves you in the guilt of treason. Persistence in it will bring you to condign punishment, to ruin, and to shame.⁵⁶

The Mormons desisted, but the nation was on the verge of its greatest crisis, the result of which was to temper the punishment for treason and to create the similar, but less odious, offense of engaging or assisting in a rebellion. Were the Confederates traitors? The South contended that secession was a right and that the secessionists were no more traitors than the embattled

⁵³ Hurst, *supra* note 31, at 807.

⁵⁴ WEYL, *op. cit. supra* note 30, at 238, 260.

⁵⁵ *Id.* at 163-86, 201-11.

⁵⁶ Proclamation of April 6, 1858, 11 Stat. (App) 796. See also WEYL, *op. cit. supra* note 30, 212-37.

patriots at Bunker Hill. The North held the view that they were insurgents and rebels, and thus could only be considered traitors. The courts resolved the problem in favor of the United States early in the war. Said the Supreme Court, "They [Confederates] . . . are none the less enemies because they are traitors."⁵⁷ A District Judge elaborated:

This is a usurpation of the authority of the federal government. It is high treason by levying war. . . . The fact that any or all engaged in the commission of these outrageous acts under the pretended authority of the legislature, or a convention of the people . . . does not change or affect the criminal character of the act. Neither South Carolina nor any other state can authorize or legally protect citizens . . . in waging war against their government, any more than the Queen of Great Britain or the emperor of France."

But holding that the Confederates were traitors, created additional problems. The mandatory sentence on conviction was death under the 1790 statute. For the occasional treason this was deemed appropriate. But now, according to the courts, there were half a million traitors under arms and many more giving them aid and assistance. It was easy to foresee a bloodbath of enormous proportions if the law was applied. Congress foresaw that the Civil War made the mandatory death penalty obsolete. Accordingly, in 1862, the law was amended to provide that henceforth the convicted traitor "shall suffer death . . . or, at the discretion of the court, he shall be imprisoned for not less than five years and fined not less than ten thousand dollars."⁵⁸ At the same time Congress also established the offense of engaging or assisting in rebellion, and authorized the seizure and sale of enemy property.⁶⁰ For engaging in or aiding rebellion the maximum punishment was established at ten years imprisonment or a fine of ten thousand dollars, or both.⁶¹

The effect of this legislation was threefold. First, it preserved the Act of 1790 prescribing the penalty of death in force for the punishment of offenses committed prior to 17 July 1862. Secondly, it punished treason committed after that date with death or fine and imprisonment unless the treason consisted of

⁵⁷ Prize Cases, 67 U.S. (2 Black) 635, 674 (1862).

⁵⁸ Charge to Grand Jury, 30 Fed. Cas. 1032, 1033 (No. 18270) (C.C.S.D. N.Y. 1861). See also United States v. Greathouse, 26 Fed. Cas. 18 (No. 15254) (C.C.N.D. Cal. 1863); United States v. Greiner, 26 Fed. Cas. 36 (No. 15262) (E.D. Pa. 1861).

⁵⁹ Act of July 17, 1862, 12 Stat. 589.

⁶⁰ 12 Stat. 589, at 590-91.

⁶¹ 12 Stat. 589, at 591.

30 MILITARY LAW REVIEW

engaging or assisting in rebellion. In the latter case it abandoned the death penalty entirely. The offense of engaging in rebellion, designed exclusively to cover the Civil War, remains in force today.⁶²

The transition of the treason act of 1790, with the graft of the 1862 statute, into the current law of treason is a problem of only minor semantics. It is sufficient for comparative purposes that the current code provision be quoted without further comment:

Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason and shall suffer death, or shall be imprisoned not less than five years and fined not less than \$10,000; and shall be incapable of holding any office under the United States.⁶³

III. TWO TYPES OF TREASON

A. *TREASON BY LEVYING WAR*

While the vast majority of the early English treason trials were concerned with the offense of compassing the King's death, some few were addressed to the problem of treason by levying war. Where the former, because of the wide construction to which it was subject, gave the courts little trouble, the latter forced the development of at least rudimentary legal concepts which could be applied with some consistency. The construction of compassing the King's demise still played a part, but an increasingly minor one. Thus while conspiring to levy, without more, was held not to constitute treason by levying war, it was still held to be compassing the King's death.⁶⁴

Participating in a rebellion aimed at the overthrow of the government or enlisting in a foreign army intending the same result seems clearly violative of this offense. Less clear is the area of riot or disorderly conduct not amounting to full scale insurgency. The case involving the tearing down of "bawdy houses" has already been cited for its unusual interpretation of "levying war."⁶⁵ The record of trial discloses that a mob of some 500, semi-organized and carrying indiscriminate weapons, not only dismantled the offending houses, but beat the constables sent to

⁶² See 18 U.S.C. § 2383 (1958).

⁶³ 18 U.S.C. § 2381 (1958).

⁶⁴ Trials of Twenty Nine Regicides, 5 How. St. Tr. 947, 984 (1660).

⁶⁵ See Trial of Peter Messenger, 6 How. St. Tr. 879 (1668).

TREASON

disperse them and shouted "Down with the red coats!" The Chief Justice saw no humor when he charged the jury:

By levying of war is not only meant, when a body is gathered together, as an army is, but if a company of people will go about any public reformation, this is High Treason, if it be to pull down inclosures, for they take upon them the regal authority; the way is worse than the thing.⁶⁴

Sir Matthew Hale dissented. He viewed the situation as nothing more serious than disorderly conduct.⁶⁷ But the English courts quickly backed off from this broad construction. Thereafter, the prosecutions for treason by levying war, arising out of domestic disturbances, were limited to such situations as where mobs acted with force to prevent the execution of a law,⁶⁸ or rioted to force the legislature to repeal an unpopular statute.⁶⁹

The United States faced a similar situation in its history. In 1794, the "Whiskey Rebellion" flared in the western counties of Pennsylvania in resistance to a tax on spirits.⁷⁰ Federal officers were first threatened, the assaulted. In July of 1794 a mob attacked the home of the chief excise officer which was defended by a number of men including 12 regulars from Fort Pitt. After a day long siege the garrison surrendered and the house was burned. Subsequently, the mob, in a show of force, marched through Pittsburgh, although no further violence developed with the garrison. The arrival of troops from Philadelphia put an end to the uprising. A number of the participants were apprehended and charged with treason. Only two persons, however, were actually brought to trial.⁷¹ In the *Mitchell* case the defense contended that the attack on the excise officer's home was an attack on him as an individual and not in his capacity as an officer of the United States, and, further that there was no attempt to resist the law on a nationwide scale. The argument was simply that this was a riot, but not treason. Justice Paterson charged the jury:

⁶⁴ *Id.* at 884.

⁶⁷ *Id.* at 911. In a time when acquittals in treason cases were notably few, six of the 14 defendants were acquitted outright and four convictions were later reversed.

⁶⁸ See Trial of Sir John Freind, 13 How St. Tr. 1 (1696).

⁶⁹ See Trial of George Gordon, 21 How. St. Tr. 485 (1781).

⁷⁰ For a full account of the incident see *United States v. Insurgents*, 27 Fed. Cas. 499 (No. 15443) (C.C.D. Pa. 1795).

⁷¹ See *United States v. Vigol*, 28 Fed. Cas. 376 (No. 16621) (C.C.D. Pa. 1795); *United States v. Mitchell*, 26 Fed. Cas. 1277 (No. 15788) (C.C.D. Pa. 1795).

30 MILITARY LAW REVIEW

If [the object of the insurrection] was to suppress the excise offices, and to prevent the execution of an act of congress, by force and intimidation, the offense, in legal estimation, is high treason; it is a usurpation of the authority of government; it is high treason by levying of war.⁷²

Both defendants were promptly convicted and sentenced to death. Both were later pardoned.⁷³

If the actions of the "Whiskey Rebels" clearly evidence a determined effort to oppose an act of Congress, those of the "Northhampton Insurgents" do not. In 1799, John Fries led a party of somewhat over 100 men to free 20 farmers being held by United States marshals for conspiracy to violate the Land Tax Act. The mob arrived at a tavern where the prisoners were being held, threatened the marshals, and secured their release. The group then promptly disbanded. No one was killed or wounded; no one was fired on, John Fries was tried for treason.⁷⁴ Charged in substantially the same language used in the *Mitchell* case, two juries returned verdicts of guilty.⁷⁵ Even in a country where the specter of revolution was still a real fear, it is difficult to conceive how Fries could have been convicted of levying war. Measured against the facts, Fries' "insurrection" appears fragmentary, momentary, and of little significance. If this was treason then almost any riot or disorder involving opposition to a law of the United States can be construed as treason. Certainly the 1962 Oxford, Mississippi, riots constituted activity far more serious than anything undertaken by Fries and his men. Weyl suggests that the trial was purely political and that Fries was a victim of a Federalist plot.⁷⁶ In any event reason prevailed and Fries was eventually pardoned.⁷⁷

Broadened by the *Fries* construction, treason by levying war was due for an even wider interpretation. By 1806, the schemes of ex-Vice President Aaron Burr began to come to light and in 1807 Burr himself was brought to trial for treason by levying war. The alleged overt acts had occurred at a place called Blennerhassett's Island in western Virginia. Yet both the prosecution and defense agreed that Burr was nowhere near the island at the time. Chief Justice Marshall, concluding that Burr's presence at

⁷² United States v. Mitchell, *supra* note 71, at 1281.

⁷³ WEYL, *op. cit.* *supra* note 30, at 85.

⁷⁴ Case of Fries, 9 Fed. Cas. 826 (No. 5126) (C.C.D. Pa. 1799); Case of Fries, 9 Fed. Cas. 924 (No. 5127) (C.C.D. Pa. 1800).

⁷⁵ *Ibid.*

⁷⁶ WEYL, *op. cit.* *supra* note 30, at 107-09.

⁷⁷ *Id.* at 109.

TREASON

that place was unnecessary, quoted with approval from the *Bollman* case:⁷⁸

It is not the intention of the court to say that no individual can be guilty of [treason] who has not appeared in arms against his country. On the contrary, if war be actually levied, that is, if a body of men be actually assembled for the purpose of effecting by force a treasonable object, all those who perform any part, however minute, or however remote from the scene of action, and who are actually leagued in the general conspiracy, are to be considered as traitors.⁷⁹

Burr was eventually acquitted. With his trial, the heyday of treason by levying war passed. Stretched to cover Fries and Burr the wide interpretation as to what constituted 'levying war' began to contract. Even as Burr sat in a Richmond courtroom, the Circuit Court in Vermont was drawing a sharp distinction between resistance to the law for a private purpose and resistance of a general character.⁸⁰ Thus the recovery by force of private property seized by a revenue agent, though accomplished by a force of about 60 men and accompanied by desultory fire between the mob and militiamen was held to be of a private character and not to constitute levying war.⁸¹ The court was also concerned about the *de minimis* aspects of this affair. "In what can we discover the treasonable mind?" asked Judge Livingston. "Can it be collected from the employment of ten or twelve muskets?"⁸² Mentioning the *Fries* case the court proceeded to emasculate its holding.

The vitality of the *Mitchell* case continued until the 1851 decision in *United States v. Hanway*.⁸³ The facts of that case leave it clear that Hanway aided one of several armed bands advocating forceable resistance to the fugitive slave law. In the immediate violence out of which the case arose a slaveowner was killed, his son wounded, and police officers attacked and beaten. Charging the jury, Justice Grier professed to see a change in the legal definition of "levying war." The "better opinion there at present" he charged, "seems to be that the term levying war should be confined to insurrection and rebellions for the purpose of over-

⁷⁸ *Ex Parte Bollman*, 8 U.S. (4 Cranch) 75 (1807).

⁷⁹ *United States v. Burr*, 25 Fed. Cas. 55, 161 (No. 14693) (C.C.D. Va. 1807).

⁸⁰ See *United States v. Hoxie*, 26 Fed. Cas. 397 (No. 15407) (C.C.D. Vt. 1808).

⁸¹ *Ibid.*

⁸² *Id.* at 399-400.

⁸³ See *United States v. Hanway*, 26 Fed. Cas. 105 (No. 15299) (C.C.E.D. Pa. 1851).

30 MILITARY LAW REVIEW

throwing the [G]overnment by force and arms. Many of the cases of constructive treason quoted [by the English writers], would perhaps now be treated merely as aggravated felonies." ⁸⁴ With this encouragement the jury promptly acquitted the accused.

Outright rebellion thus continued to come within the area defined by the term "levying war." The Civil War appeared to some to be the opportunity to utilize this term to prosecute the Confederates for treason. As a matter of record, however, only a few indictments arose out of that war, and these produced lenient results. The sentences of Ridgely Greathouse and his compatriots, for example, convicted of levying war by attempting to outfit a privateer for Confederate service were terminated upon their taking the oath of allegiance to the United States.⁸⁵ The indictments against such contrasting individuals as Charles Greiner,⁸⁶ a member of a Georgia artillery company which participated in the seizure of Fort Pulaski, and Jefferson Davis,⁸⁷ President of the Confederate States, were never brought to trial.

Since that time, a number of incidents have occurred which might have been considered a basis for charges of treason by levying war. The activity of the Klan during Reconstruction, the Haymarket Riots of 1886, and the march of the Bonus Army in 1932 were all serious enough to require the dispatch of troops to maintain law and order. But the definition which limits treason by levying war to actual rebellion against the Government seems to have prevailed. It is significant that since the *Davis* case not one attempt has been made to revive the offense.

B. TREASON BY ADHERING TO THE ENEMY GIVING HIM AID AND COMFORT

Unlike the offense of treason by levying war which passed from the scene almost one-hundred years ago, the offense of treason by adhering to the enemy has achieved a considerably longer and more useful existence. This phase of treason encompasses two elements: adhering to the enemy and giving him aid and comfort. With these elements the problem of intent is inexorably intertwined. A citizen may intellectually, emotionally

⁸⁴ *Id.* at 127.

⁸⁵ *United States v. Greathouse*, 26 Fed. Cas. 18 (No. 15524) (C.C.N.D. Cal. 1863).

⁸⁶ See *United States v. Greiner*, 26 Fed. Cas. 36 (No. 15262) (D.C.E.D. Pa. 1861).

⁸⁷ See *Case of Davis*, 7 Fed. Cas. 63 (No. 3621a) (C.C.D. Va. 1867-1871).

and spiritually sympathize with the enemy. He may harbor disloyal thoughts, But so long as he fails to engage in some sort of conduct designed to give the enemy aid and comfort, the crime of treason is not complete.⁸⁸ Conversely a citizen may do an act which gives the enemy aid and comfort, but if there is no adherence to the enemy's cause there is no treason.⁸⁹ By doing the act he may appear outwardly a traitor but he is not legally a traitor.⁹⁰ Nor does it appear necessary that the enemy wants or needs the proffered assistance. The mere fact that it is offered or rendered with the requisite intent will make the crime complete.

As in other aspects of the law, we must go back to England for a starting point. Interwoven throughout the English cases is the conception that adhering to the enemy necessarily compassed the death of the king. For that reason, indictments for aiding the enemy, in and of itself, are scarce. But at least as early as 1691 it was recognized as a separate offense.⁹¹ At the trial of Sir Richard Grahme for attempting to smuggle out of England a number of documents concerning the status of military defenses, Lord Chief Justice Holt, after commenting on the indictment for compassing the King's death, observed: "There is another treason in the indictment mentioned and that is for adhering to, and abetting the king's enemies, there being open war declared between the king and queen and the French king."⁹²

Defining the rationale of the offense the Solicitor General of England argued in 1781:

How can any state exist, how contend with an enemy, if it is to suffer within its own bosom men employed to give intelligence of all its operations to those with whom it is at war? One man, so employed, may often times do much more mischief to the country of whose operations he gives intelligence than an army of 50,000 men."

The English courts also established the proposition that the offense was complete once the overt act occurred and it was no defense that the enemy was not actually aided.⁹⁴ The conviction of Viscount Preston was sustained notwithstanding that his attempt to smuggle defense plans out of England was terminated

⁸⁸ *Cramer v. United States*, 325 U.S. 1 (1944); *United States v. Werner*, 247 Fed. 708 (E.D. Pa, 1918), *aff'd* 251 U.S. 466 (1919).

⁸⁹ See *Kawakita v. United States*, 343 U.S. 717 (1952).

⁹⁰ *United States v. Werner*, 247 Fed. 708 (E.D. Pa. 1918), *aff'd* 251 U.S. 466 (1919).

⁹¹ See *Trial of Sir Richard Grahme*, 12 How. St. Tr. 645 (1691).

⁹² *Id.* at 730.

⁹³ *Trial of F. H. DeLa Motte*, 21 How. St. Tr. 687, 798 (1781).

⁹⁴ See *Trial of Sir Richard Grahme*, 12 How. St. Tr. 645 (1691).

30 MILITARY LAW REVIEW

by his apprehension.⁹⁵ Nor did it avail those accused of treason by attempting to mail secrets abroad in time of war to contend that the letters were intercepted before they left the country.⁹⁶ The celebrated trial of Captain Thomas Vaughan resulted in the conviction for aiding the enemy of a seaman who went "cruising" under a French commission where there was no evidence that he made any hostile attempt upon an English vessel.⁹⁷

All of these cases have been cited by American courts. Perhaps the leading case in the United States involves the efforts of Max Haupt to acquire a job for his son, a Nazi secret agent, at a factory engaged in producing lenses for the top-secret Norden bombsight. The efforts consisted solely of visiting the homes of a plant superintendent and a shop foreman and inquiring into the means of securing such employment. There was no evidence that a job application was ever submitted or that any further step was taken in that direction.⁹⁸ Affirming the conviction, Mr. Justice Jackson commented succinctly:

His acts aided an enemy of the United States toward accomplishing his mission of sabotage. The mission was frustrated but the defendant did his best to make it succeed. [That] His overt acts were proved in compliance with the hard test of the Constitution, are hardly denied and the proof leaves no reasonable doubt of the guilt.⁹⁹

While not necessary to the result, this principle was expressly adhered to in the case of radio propagandist, Douglas Chandler.¹⁰⁰ The evidence established that Chandler had prepared a number of broadcasts for the use of the German Radio Broadcasting Company. Chandler contended there was no evidence any of the recordings were ever used, or if used, that anyone in the United States ever heard them. Dismissing this argument the court concluded:

It does not even matter whether the particular recordings . . . were actually broadcast. Chandler's service was complete with the making of the recordings, which became available to the enemy to use as it saw fit. . . . His act of making the recording for the enemy is like giving to an enemy agent a paper containing military information, which would

⁹⁵ *Ibid.*

⁹⁶ Trial of David Tyrie, 21 How. St. Tr. 815 (1782); Trial of Florence Hensey, 19 How. St. Tr. 1342 (1758).

⁹⁷ Trial of Captain Thomas Vaughan, 13 How. St. Tr. 485 (1696).

⁹⁸ For a detailed discussion of the evidence in this regard, see *United States v. Haupt*, 152 F.2d 771 (7th Cir. 1945) *aff'd*, 330 U.S. 631 (1947).

⁹⁹ *Haupt v. United States*, 330 U.S. 631, 644 (1947).

¹⁰⁰ *Chandler v. United States*, 171 F.2d 921 (1st Cir.), *cert. denied*, 336 U.S. 918 (1948).

be a completed act of aid and comfort, though the enemy agent later lost the paper and thus never put the information to any effective use.¹⁰¹

Who is the "enemy" for the purpose of receiving this aid and adherence? In the English cases, oriented as usual with monarchical concepts, it was the foreign sovereign himself. The early American cases immediately following the Revolution departed from this concept. One early Pennsylvania case charged the defendant with intending "... to raise again and restore the Government and tyranny of the King of Great Britain. . . ." ¹⁰² However, reference to the king, as such, played an increasingly lesser role and prosecutions were based merely on aid to his soldiers.¹⁰³

An opportunity to fully explore the definition of an "enemy" did not arise until the Civil War. The problem quickly arose as to whether the Confederates were "enemies" for the purpose of the treason law. The problem was resolved in the negative by Mr. Justice Field in the *Greathouse* case.¹⁰⁴ He charged the jury:

The term "enemies" as used in the second clause, [of the Constitutional provision] according to its settled meaning, at the time the constitution was adopted, applies only to the subjects of a foreign power in a state of open hostility with us. It does not embrace rebels in insurrection against their own government. An enemy is always the subject of a foreign power who owes no allegiance to our government or country.¹⁰⁵

The practical result was that all future treason prosecutions against the Confederates had to be charged ("levying war." ¹⁰⁶ It is interesting to note, and practical politics appears to have dictated, that the definition of an "enemy" for the purpose of treason and that for the purpose of confiscating the property of an "enemy" received diametrically opposite treatment. In the latter situation the courts had no problem holding Confederate soldiers and citizens to be enemies and their property subject to forfeit.¹⁰⁷

¹⁰¹ *Id.* at 941.

¹⁰² *Republica v. Carlisle*, 1 U.S. (1 Dall.) 35 (1778).

¹⁰³ *Republica v. Malin*, 1 U.S. (1 Dall.) 33 (1778); *accord*, *United States v. Hodges*, 26 Fed. Cas. 332 (No. 15374) (C.C.D. Md. 1815).

¹⁰⁴ *United States v. Greathouse*, 26 Fed. Cas. 18 (No. 15254) (C.C.N.D. Cal. 1863).

¹⁰⁵ *Id.* at 22.

¹⁰⁶ *But cf.* *Prize Cases*, 67 U.S. (2 Black) 635 (1862) which seems to accord the Confederacy belligerency status although for a different purpose (i.e., violating the blockade).

¹⁰⁷ *The Venice*, 69 U.S. (2 Wall.) 258 (1864); *Mrs. Alexander's Cotton*, 69 U.S. (2 Wall.) 404 (1864).

30 MILITARY LAW REVIEW

The offense of treason by aiding the enemy can only be committed during time of war.¹⁰⁸ But it does not necessarily follow that the war must be attired with all the customary trimmings, such as a formal declaration. It is true as a matter of fact that all previous treason prosecutions in this area have arisen out of incidents which occurred during time of a formally declared conflict. For this reason, it is perhaps unfortunate that no treason prosecution followed the Korean conflict by which the standards of that "war" could be tested. Some support for the proposition that less than a "formal" war will suffice may be found in an Attorney General's opinion in 1798, during the maritime dispute with France, that the treason law applied to a French citizen who was in the United States buying supplies for French bases in the West Indies.¹⁰⁹ Again, in 1871, the Attorney General expressed the opinion that persons apprehended running guns and ammunition to hostile Indians were subject to military court-martial for "relieving the enemy."¹¹⁰

Today a practical question may be raised concerning the status of the Viet Cong. Are they an "enemy" as that word is used in the treason statute? This question has recently received collateral consideration with the decision to issue certain awards for valor in combat in South Vietnam. Fearing that the term "enemy" might be legally inapplicable,¹¹¹ Congress amended the statutes governing the award of the Medal of Honor, Distinguished Service Cross and Silver Star to include situations where American servicemen were in conflict with an opposing foreign force or serving with a friendly foreign force engaged in an armed conflict.¹¹² Yet when it awarded the Medal of Honor to Captain Roger Donlon, the Department of the Army had no hesitancy in referring to the Viet Cong as an "enemy" on fire occasions.¹¹³

While the cited authorities do not fully resolve the question, they may be taken to indicate that the civil offense of treason and its military counterpart of aiding the enemy could well be committed in an escalated "cold war" situation.

¹⁰⁸United States v. Fricke, 259 Fed. 673 (S.D.N.Y. 1919).

¹⁰⁹ See 1 OPS. ATT'Y GEN. 49 (1798).

¹¹⁰ See 14 OPS. ATT'Y GEN. 470 (1871).

¹¹¹ 1963 U.S.C. CONG. & AD. NEWS 776.

¹¹² See 10 U.S.C. §§ 3741, 3742, 3746 (Supp. V, 1964).

¹¹³ See Gen. Orders No. 41, Hq. Dept. of Army (17 Dec 1964).

IV. THE JURISDICTIONAL ASPECTS OF TREASON

A. OVERSEAS TREASON BY AMERICAN NATIONALS

No one would suggest that the prosecution of a native or naturalized American citizen for treason committed within the borders of the United States would raise a jurisdictional problem. But treason committed overseas is a different matter. The law punishes as traitors those who adhere to the enemies of the United States within the country or elsewhere.¹¹⁴ Where the law is applied to American citizens, it is the "or elsewhere" that raises the problem. It is a problem of recent origin. For once we are unable to glean from the State Trials any case dealing with overseas treason,¹¹⁵ and history has shown it to be basically an American problem. True, England produced Casement,¹¹⁶ but the evidence in the Joyce case strangely points to the fact that even "Lord Haw Haw" was an American national.¹¹⁷

At the outset, it may be well to consider where the concept of overseas treason originates. Normally the answer would be found in the Constitution. It has been noted that treason is the only crime defined in that document. But a re-reading of Article 3, section 3, fails to disclose the words "or elsewhere." The convention that framed the Constitution certainly considered them. Its members were familiar with the statute of Edward III.¹¹⁸ Yet the words do not appear in the draft submitted by the Committee of Detail,¹¹⁹ and a proposed substitute which would have included them was defeated by an 8 to 2 vote.¹²⁰ The words first appear in the statute by which Congress implemented the authority given it to declare the punishment for treason.¹²¹

It follows that one objection to the inclosure of the words "or elsewhere" in this statute is that the power of Congress is limited

¹¹⁴ 18 U.S.C. § 2381 (1958).

¹¹⁵ Unless you consider the *Vaughan* case involving treason on the high seas. Case of Captain Thomas Vaughan, 13 How. St. Tr. 485 (1696).

¹¹⁶ An Irish revolutionary who attempted to carve out an independent Ireland with German help during World War I. On his return from Germany he was captured, tried for treason, and executed. See *Rex v. Casement*, 115 L.T.R. (N.S.) 267 (1917).

¹¹⁷ *Rex v. Joyce*, 173 L.T.R. (N.S.) 377 (1945), *aff'd sub nom. Joyce v. Director of Public Prosecutions*, 174 L.T.R. (N.S.) 206 (1946). See also WEST, *THE NEW MEANING OF TREASON* (1964).

¹¹⁸ 2 FARRAND, *RECORDS OF THE FEDERAL CONVENTION OF 1787*, at 345 (1937).

¹¹⁹ *Id.* at 182

¹²⁰ *Id.* at 347-48.

¹²¹ Act of April 30, 1790, 1 Stat. 112.

30 MILITARY LAW REVIEW

to providing the punishment for treason and does not extend to declaring where the offense may be committed. A second argument is that the words "or elsewhere" qualify only the phrase "giving aid and comfort" and do not apply to the phrase "adheres to." If this were true and both the adherence and the aid and comfort to the enemy took place outside the United States the statute would not be violated.

Both of these contentions were unsuccessfully asserted in the *Chandler case*.¹²² With regard to the former the court replied that had the framers intended to restrict the crime to the United States, they could easily have done so.¹²³ Furthermore, the restrictive words "within their territories" had been deliberately rejected by the Committee of the Whole.¹²⁴ The latter contention too was rejected, the court concluding that such theory ". . . violates the plain language of the statute."¹²⁵

If this proposition can be considered as firmly settled, what recourse is open to the American overseas who chooses to support his country's enemy? The Nationality Act of 1940 opened the door: voluntary expatriation.¹²⁶ Prior to that statute wartime expatriation was prohibited,¹²⁷ but this restriction was eliminated in the new legislation. Among the recognized means by which nationality could be lost were (a) obtaining naturalization in a foreign state, (b) taking the oath or making a formal declaration of allegiance to a foreign state, or (c) making a formal renunciation of United States citizenship before a diplomatic or consular official of the United States in a foreign state.¹²⁸

How many Americans took advantage of the Nationality Act to transfer their allegiance to a wartime enemy and thus avoided post-war prosecution for treason is unknown. A Federal Court has used the phrase "many persons."¹²⁹ One writer has gone vo

¹²² United States v. Chandler, 72 F.Supp. 230 (D. Mass. 1947), *aff'd*, 171 F.2d 921 (1st Cir. 1948), *cert. denied*, 336 U.S. 918 (1949).

¹²³ 171 F.2d at 929.

¹²⁴ 2 FARRAND, *op. cit.* *supra* note 118, at 347-48.

¹²⁵ United States v. Chandler, 72 F.Supp. 230, 233 (D. Mass. 1947), *aff'd*, 171 F.2d 921 (1st Cir. 1948), *cert. denied*, 336 U.S. 918 (1949); *accord*, *Gillars v. United States*, 182 F.2d 962 (D.C. Cir. 1950), *Best v. United States*, 184 F.2d 131 (1st Cir.), *cert. denied*, 340 U.S. 939 (1950).

¹²⁶ Nationality Act of 1940, § 401, 54 Stat. 1137.

¹²⁷ Act of March 2, 1907, 34 Stat. 1228.

¹²⁸ Nationality Act of 1940, § 401, 54 Stat. 1137.

¹²⁹ See *D'Aquino v. United States*, 192 F.2d 338, 348 (9th Cir.), *cert. denied*, 343 U.S. 935 (1951).

far as to assert that "several thousand" changed allegiance to Japan alone.¹³⁰ At least three were unsuccessful.

On December 8, 1941, approximately simultaneously with the declaration of war, Mildred Gillars, better known as "Axis Sally" executed a paper which contained the words "I swear my allegiance to Germany." The paper was then given to her superior. On the basis of this document, which was never produced, she urged the jury be instructed that if they found this to be a sufficient renunciation of citizenship, they must acquit. The court refused to give the instruction and the conviction was affirmed on appeal.¹³¹ A loose interpretation of the statute might have sustained appellant's contention, but the court chose to require strict compliance. The court noted there was no evidence that the paper had been sworn to before anyone or that there was any connection between it and any procedure having to do with obtaining Reich citizenship.¹³² Nor did it find any substance to appellants' contention that her citizenship had ceased when her United States passport, submitted for renewal in 1941, had been retained by the consular agent. A passport is some evidence of citizenship, it is indeed useful in travel, but, concluded the court, its absence does not deprive an American of his citizenship.¹³³

A second argument advanced in favor of successful expatriation under the Nationality Act of 1940 was advanced by Iva D'Aquino, the "Tokyo Rose" of the Pacific theater. She noted that under the expatriation provisions of the act a person was permitted to shed his allegiance to the United States and by so doing could engage in adherence, aid and comfort to the enemy with impunity.¹³⁴ She argued that to try her for treason for acts which the law permitted others to do was unreasonable and arbitrary and constituted a denial of due process under the Fifth Amendment.¹³⁵ But the court found no sound basis for such contention and concluded it was no more than a mere "...play on words."¹³⁶ The Constitutional argument got no further than the effort to give the statute a broad construction.

¹³⁰ See Blakemore, *Recovery of Japanese Nationality as Cause for Expatriation in American Law*, 43 AM. J. INT'L L. 441, 451 (1949).

¹³¹ Gillars v. United States, 182 F.2d 962 (D.C.Cir. 1950).

¹³² *Id.* at 983.

¹³³ *Id.* at 981.

¹³⁴ See D'Aquino v. United States, 192 F.2d 338, 348 (9th Cir.), cert. denied, 343 U.S. 935 (1951).

¹³⁵ See *ibid.*

¹³⁶ See *id.* at 349.

30 MILITARY LAW REVIEW

One last problem area in the field of overseas treason concerns the status of the dual citizen. Such an individual was Toyoma Kawakita.¹³⁷ Born in California of Japanese parents who were citizens of Japan, he was thus a citizen of the United States by birth, and, by Japanese law, a citizen of Japan. In 1939, he visited Japan on an American passport to attend college. When the war broke out he chose to stay in Japan and finish his education. During this period he was registered by the Japanese police as an alien. Subsequently, he attempted to renounce his American citizenship. To do this he had his name entered on a family census register. He then obtained employment with a metal company where he was assigned as translator in connection with the use of American prisoners of war as laborers. Not content with a passive role he continually humiliated the captives and frequently subjected them to brutal treatment. In 1946, he reappplied for his American passport and returned to the United States. A chance recognition by a former prisoner caused his arrest and subsequent trial for treason. On appeal Kawakita stressed his Japanese nationality. In addition to the entry of his name in the family register, he argued for the broader proposition that an individual possessing dual nationality who resides in one of the countries of which he is a national cannot be guilty of treason against the other country.¹³⁸ The assertion appears to be based on the "right" of a dual national to make an election, in time of war, to which of his sovereigns he will adhere. The court promptly rejected his contention. Concerning the contention that Kawakita, by his acts, had renounced his American citizenship the court answered:

That conclusion is hostile to the concept of citizenship as we know it, and it must be rejected. One who wants that freedom can get it by renouncing his American citizenship. He cannot turn it into a fair-weather citizenship, retaining it for possible contingent benefits but meanwhile playing the part of the traitor. An American citizen owes allegiance to the United States wherever he may reside.¹³⁹

As regards the family register, the court dismissed this contention on the theory that the registration was merely as assertion of some of the rights Kawakita already possessed by reason of his dual nationality.

The *Kawakita* holding is far from decisive. It is a minority

¹³⁷ See *Kawakita v. United States*, 96 F.Supp. 824 (S.D.Cal. 1950), *aff'd*, 190 F.2d 506 (9th Cir.), *aff'd*, 343 U.S. 717 (1951).

¹³⁸ See *Kawakita v. United States*, 343 U.S. 717, 732 (1951).

¹³⁹ *Id.* at 735.

opinion. Two justices took no part in the decision and three dissented.¹⁴⁰ The dissent is based on the conclusion that by his acts Kawakita had expatriated himself as well as he could have.¹⁴¹ Blakemore appears to make even a more telling point. He discusses the unusual Japanese law of "recovery" of nationality and concludes that any person who so "recovers" under Japanese law has effectively expatriated himself under the Nationality Act of 1940.¹⁴² Since "recovery" under Japanese law may be accomplished through inclusion in the Family Register Record, Kawakita can thus be said to have expatriated himself prior to the time of his treasonous acts.

It may be concluded, then, that an American may avoid his natural loyalty to his country through an act of voluntary expatriation. But the mere fact that such person purports to verbally or informally renounce his citizenship or purports to pledge his allegiance to any enemy state, without complying with its formal requirements, will not excuse the crime of treason. Before allowing a citizen to adhere to our enemies the courts will demand a strict compliance with the statutes dealing with expatriation even for a person with a dual nationality status. The "highest of all crimes" cannot be lightly evaded.

B. TREASON BY RESIDENT ALIENS

If treason by an American citizen must be either black or white, then treason by a resident alien can only be described as gray. The allegiance owed by a citizen is fixed and certain; that owed by an alien imperfect and temporary. If the nationality of the alien is that of an enemy belligerent the problem is increased. The alien may feel no love for the country in which he resides; he is more likely than its native son to wish it ill, but if he commits one overt act designed to accomplish its downfall, the noose looms just as high.

The underlying rationale behind punishing the alien for treason against the host country is not new. It was firmly established in England. It was clearly expressed in 1781 by Mr. Justice Butler, in passing the "usual" sentence upon one DeLa Motte, a Frenchman living in England who had attempted to send military secrets to aid his homeland, as follows:

During your residence in this country, as well as during the course of

¹⁴⁰ See *id.* at 745.

¹⁴¹ See *id.* at 746.

¹⁴² See Blakemore, *supra* note 130, at 449.

30 MILITARY LAW REVIEW

your trial, you have received the protection of the laws of the land. As such you owed a duty to those laws, and an allegiance to the king whose laws they are; but you have thought it fit to abuse that protection you have received."

The adoption of this principle in American law appears clear although the actual trial of an alien for treason is unknown in this country. It has already been observed that the Attorney General in an early opinion, concluded that a French citizen in this country was subject to trial for treason.¹⁴⁴

Further support for the general principle may be found in *The Pizzaro*.¹⁴⁵ The question concerned whether or not an English citizen could be the "subject" of the King of Spain, for treaty purposes, where his ship had been seized by an American privateer during the War of 1812. Holding that he could, Justice Story, referring to the location of that citizen's actual residence, concluded:

... a person domiciled in a country, and enjoying the protection of its sovereign, is deemed a subject of that country. He owes allegiance to the country, while he resides in it; temporarily indeed, . . . but so fixed that, as to all other nations, he follows the character of that country, in war as well as in peace."¹⁴⁶

With the outbreak of the Civil War zealous judges, foreseeing a rash of impending treason trials, charged their grand juries in

¹⁴⁴ Trial of DeLa Motte, 21 How. St. Tr. 687, 814-815 (1781).

¹⁴⁵ See 1 OPS. ATTY. GEN. 49 (1798). It can be argued that his holding is inconsistent with the decision in *United States v. Villato*, 2 U.S. (2 Dall.) 370 (1797), a trial for treason of an alleged American sailor who joined the crew of a French vessel which subsequently captured an American ship. At the trial the accused successfully contended that he was not an American citizen but a Spaniard. Arguing on the merits the U.S. Attorney conceded "that if the prisoner is not a nationalized citizen of the United States, he must be discharged," *United States v. Villato*, *supra* at 371. In the subsequent holding both judges concurred that since the accused was found not to be a citizen of the United States he must "consequently be released from the charge of high treason." *United States v. Villato*, *supra* at 373. Given broad interpretation these words can be read to mean that no foreigner can be tried for treason. But as the acts were committed on the high seas it is more reasonable to conclude that the place of the acts must have been considered by counsel and the court, and not as suggesting that a resident alien could not be found guilty. It has never been suggested that a foreigner who aids our enemy overseas can be brought himself within our treason law. It is significant that no subsequent effort has been made to give this language a wider construction.

¹⁴⁶ 15 U.S. (2 Wheat.) 227 (1817).

¹⁴⁷ *Id.* at 246. It is unfortunate that Justice Story used the words "domiciled" and "resides" interchangeably since the former implies an intent to remain.

detail with the law of the offense.¹⁴⁷ Only one of these specifically included instructions concerning resident aliens but it specifically adhered to the English rule, charging that any such sojourner, enjoying the protection of the United States, owes a local allegiance, and may be guilty of treason by cooperating with rebels or foreign enemies.¹⁴⁸

Only one case arising out of that conflict seems to have considered the problem of treason by resident aliens,¹⁴⁹ but that case is significant in its adherence to the English rule. The suit involves an effort to recover damages for goods owned by British citizens which were seized in Alabama by United States forces. The court discusses the loyalty owed by a resident alien in this language:

The alien, whilst domiciled in the country, owes a local and temporary allegiance, which continues during the period of his residence. This obligation of temporary allegiance by an alien resident in a friendly country is everywhere recognized by publicists and statesmen. . . . [I]t is well known that, by the public law, an alien or a stranger born, for so long a time as he continues within the dominions of a foreign government, owes obedience to the laws of that government, and may be punished for treason or other crimes as a native born subject might be. . . .¹⁵⁰

Thus, another of the English rules has been assimilated into the American law of treason. As with many others it can at times be considered harsh. Certainly the *Carlisle* case can be read for the proposition that Carlisle could have been convicted of treason as a resident alien. The rationale behind such prosecution would have been that the alien was enjoying the protection of the laws of the United States. Yet Carlisle was deep in Alabama where the laws of the United States protected him about as well as they could have in Africa. Consider also the case of the alien whose homeland has become the "enemy." Does his duty to his country extend to working for its success in the state where he resides? If he does so he subjects himself to a treason prosecution by that state. But the rule is harsh where tested by the needs of the individual. Tested by the needs of the state it becomes necessary in the interest of national self-protection.

¹⁴⁷ See, e.g., Charge to Grand Jury, 30 Fed. Cas. 1032 (No. 18270) (C.C. S.D. N.Y. 1861); Charge to Grand Jury, 30 Fed. Cas. 1036 (No. 18272) (C.C.S.D. Ohio 1861).

¹⁴⁸ Charge to Grand Jury, 30 Fed. Cas. 1039 (No. 18273) (D. Mass. 1861); cf. Charge to Grand Jury, 30 Fed. Cas. 1047 (No. 18276) (C.C. E.D. Pa. 1851).

¹⁴⁹ See *Carlisle v. United States*, 83 U.S. (16 Wall.) 147 (1872).

¹⁵⁰ *Id.* at 154-55. Note again the words "domiciled" and "residence" are used interchangeably.

V. AFFIRMATIVE DEFENSES

A. IN GENERAL

Will anything negate the crime of treason? With a survey of the English cases as a guide it is tempting to answer in the negative. For hundreds of years head after head rolled from the Tyburn block after trials which were little more than formality, and under circumstances where an acquittal could be dangerous for the jury.¹⁵¹ In such a setting any affirmative defense was doubly dangerous since the very nature of such defense admits the acts complained of but seeks to excuse or justify them by attacking some other element of the offense. It is not surprising, therefore, that all but a scattered few chose to plead not guilty and, with the law against them, endeavor to argue the facts.

Of those few who have attempted to assert affirmative defenses some have bottomed their reliance on grounds of lack of citizenship.¹⁵² One notable exception, and a study in the futility of it all, was the celebrated case of Sir Walter Raleigh.¹⁵³ Tried in 1603, Raleigh was convicted of treason by plotting rebellion. His sentence to death was suspended and he languished in prison for 14 years. Subsequently he was released and commissioned to lead a military expedition to Guiana which involved fighting with the Spanish. By the time he returned to England the political situation had shifted and England was currying favor with Spain. The Spanish minister demanded his execution. Not knowing any offense to try him for, the authorities decided merely to vacate the old suspended death sentence and execute Raleigh for treason. He urged in vain that the Commission from the king had amounted to a pardon.¹⁵⁴ A former Lord Chancellor and most of the lawyers in England agreed with him.¹⁵⁵ Nevertheless the Lord Chief Justice ruled otherwise.¹⁵⁶ The pardon must be specific, he held, it could not be implied. Raleigh went to the block. Constructive treason was a one edged sword; it cut only in favor of the prosecution.

¹⁵¹ Following the acquittal of Sir Nicholas Throckmorton, 1 How. St. Tr. 869 (1554), an enraged judge ordered the jury imprisoned and subsequently fined them heavily.

¹⁵² See notes 114-49 *supra*, and text accompanying.

¹⁵³ Trial of Sir Walter Raleigh, 2 How. St. Tr. 1 (1603).

¹⁵⁴ *Id.* at 34.

¹⁵⁵ *Ibid.*

¹⁵⁶ To further point up the hopelessness of the situation it should be noted that the Lord Chief Justice was none other than Sir Edward Coke, who had prosecuted Raleigh at the original trial.

Other efforts at raising affirmative defenses have faced equally bleak results. Drunkenness has been raised, but evidence that the defendant was in a state of ambulatory stupefaction has been considered insufficient to establish a defense to a charge of treason by resisting law officers.¹⁵⁷ Nor may the motive of the accused, that he genuinely believes what he does is in the best interests of his country, be raised as bearing on his intent to aid the enemy.¹⁵⁸ While insanity has been recognized as a defense to treason, only one case has been found where it was successfully argued.¹⁵⁹ One affirmative defense has been raised consistently enough to be treated separately. That defense is duress, the deprivation of an individual's free will to act.

B. DURESS

The defense of duress was first fully considered following the rebellion of 1745 that came to grief at the Battle of Culloden. Alexander MacGrowther had participated in that rebellion. At his trial, witnesses testified that he had been seen on several occasions with the rebel army and wearing its uniform.¹⁶⁰ MacGrowther asserted, however, that he had been a most unwilling participant. He had joined the rebel army, this he conceded. But, he contended, he had done so only after the Duke of Perth, in whose regiment he had served, had threatened to burn the houses and destroy the crops of any of his tenants who desisted. Even with this, MacGrowther argued, he had hesitated, until he was told he would be forceably bound and taken along anyway.¹⁶¹ Lord Chief Justice Lee was not persuaded. He instructed the jury: "[T]he fear of having houses burnt, or goods spoiled, . . . is no excuse for joining and marching with rebels. The only force that doth excuse, is a force upon the person, and present fear of death; and this force and fear must continue all the time the party remains with the rebels."¹⁶² MacGrowther was found guilty but his argument was not entirely unsuccessful for he was later reprieved.

While a shortened version of the *MacGrowther* rule was cited as *dicta* in the *McCarty* case,¹⁶³ it was first given serious consid-

¹⁵⁷ See *Trial of George Purchase*, 15 How. St. Tr. 651 (1710).

¹⁵⁸ *Best v. United States*, 184 F.2d 131 (1st Cir.), cert. denied, 340 U.S. 939 (1950).

¹⁵⁹ See *Trial of James Hadfield*, 27 How. St. Tr. 1281 (1800).

¹⁶⁰ *Trial of Alexander MacGrowther*, 18 How. St. Tr. 391, 392 (1746).

¹⁶¹ *Id.* at 393.

¹⁶² *Id.* at 394.

¹⁶³ *Respublica v. McCarty*, 2 U.S. (2 Dall.) 86 (1781).

30 MILITARY LAW REVIEW

eration in this country in *United States v. Vigol*,¹⁶⁴ one of the cases growing out of the Whiskey Rebellion. Vigol's contention seems to have been more that he was caught up in the spirit of things than that he was actually forced to participate. His defense found no favor with Justice Patterson who instructed the jury in words similar to those employed by Lord Chief Justice Lee some 50 years earlier. Commenting on the reason behind the rule the judge stated:

If indeed such circumstances [apprehension of something less than immediate fear of death] could avail, it would be in the power of every crafty leader of tumults and rebellion, to indemnify his followers, by uttering previous menaces; an avenue would be forever open for the escape of unsuccessful guilt; and the whole fabric of society must inevitably, be laid prostrate."¹⁶⁵

A vigorous assault on the *MacGrowther* rule was leveled in 1815 by William Pinkney, attorney for John Hodges who was tried for treason for returning four British stragglers who had been taken prisoner during the British withdrawal from Washington in the war of 1812.¹⁶⁶ It appeared that the British had threatened to burn the town of Upper Marlboro and hold women and children hostages until the men were returned. Pinkney stressed the military severity of the situation in an eloquent speech. He argued:

[T]he enemy were in complete power in the district. . . . They were unawed by the thing which we called an army, for it had fled in every direction. They were omnipotent. . . . They menaced pillage and conflagration; and after they had wantonly destroyed edifices which all civilized warfare had hitherto respected, was it to be believed that they would spare a petty village, which had renewed hostilities, before the seal of its capitulation was dry? There was menace; power to execute; probability, nay, certainty, that it would be executed. How, then, can you find a wicked and traitorous motive in the breast of my client?¹⁶⁷

Given weak instructions by an uncertain court the jury agreed with Pinkney, and "without hesitating a moment," returned a finding of "not guilty."¹⁶⁸

The *Hodges* case appears to represent a departure from the *MacGrowther* rule. If so, it was only temporary. The Civil War brought a prompt re-recognition of the rule,¹⁶⁹ which has been

¹⁶⁴ 2 U.S. (2 Dall.) 346 (1795).

¹⁶⁵ *Id.* at 347.

¹⁶⁶ *United States v. Hodges*, 26 Fed. Cas. 332 (No. 15374) (C.C.D. Md. 1815).

¹⁶⁷ *Id.* at 335.

¹⁶⁸ *Id.* at 336.

¹⁶⁹ See *United States v. Greiner*, 26 Fed. Cas. 36, 39 (No. 15262) (E.D. Pa. 1861).

TREASON

reasserted to this day. If any relaxation of the rule can be found in the *Gillars* case,¹⁷⁰ it is only to the extent that the coercion or compulsion has been extended from threat of immediate death to include threat of immediate serious bodily injury. This can hardly be considered the opening of a door.

Only one more case need detain us. In the trial of "Tokyo Rose" the defense conceded that the rule announced in *Gillars* was correct where applied within the United States, but argued that it was an unsatisfactory rule when the accused was in an enemy country, for in such situations he was unable to get protection from the United States and the compulsion was on the part of the enemy government itself.¹⁷¹ Recognizing that this might hold true for an individual conscripted into the enemy army, the court responded:

We know of no rule that would permit one who is under the protection of an enemy to claim immunity from prosecution for treason merely by setting a claim of mental fear of possibly future action on the part of the enemy."

Thus it has been seen that while the legal rule on duress as applied to treason seems strict on its face, it has not been harsh in application. Where the threat has proved real enough the courts have not been harsh on the individual affected even though the threat has been less than that required to excuse him by law. The United States citizen, as does its soldier, owes his country a determination to resist by all means within his power, and only when he has been brought to the last ditch of resistance may he save his life at the temporary expense of that duty.

VI. THE MILITARY LAW OF TREASON

The Trial Counsel addressed the court: "If any member of the court or the law officer is aware of any facts, which he believes may be a ground for challenge by either side against him, he should now state such facts." A Lieutenant turned to the Law Officer: "Sir, I challenge myself on the grounds that I am hostile to the accused and that prior to the convening of this court I have formulated the opinion and expressed the opinion that the accused is a traitor."¹⁷²

¹⁷⁰ *Gillars v. United States*, 182 F.2d 962, 976 (D.C. Cir. 1950).

¹⁷¹ *D'Aquino v. United States*, 192 F.2d 338 (9th Cir.), cert. denied, 343 U.S. 935 (1951).

¹⁷² *Id.* at 359.

¹⁷³ Statement of Lt. Schowalter, disqualifying himself as a member of the court. *United States v. Batchelor*, 7 U.S.C.M.A. 354, 362, 22 C.M.R. 144, 152 (1956).

30 MILITARY LAW REVIEW

But "treason *as such* is not an offense properly cognizable by a court-martial." These are the words of no less of an authority than Colonel Winthrop.¹⁷⁴ Yet almost immediately the effect of this conclusion becomes blurred. It is for an excellent reason that Winthrop italicizes the words "*as such*." All will readily admit that the word "treason" has never appeared in the articles of war which, since 1776, have governed the armies of the United States. Yet Winthrop feels compelled to explain that the articles concerning relieving and communicating with the enemy are "reasonable in their nature" and he quotes with approval such definitions of the offenses as "overt acts of treason" and "closely allied to treason."¹⁷⁵ The Colonel concludes: "Whenever, therefore, an overt act of the class specified in these Articles gives substantial aid and comfort to the enemy, and thus evidences, so far forth, an adherence to his cause, it can scarcely be regarded as less than an act of treason."¹⁷⁶

The two articles of war referred to by Winthrop have subsequently synthesized into the present Article 104 of the *Uniform Code of Military Justice* which defines the offense as follows:

Any person who—

(1) aids, or attempts to aid, the enemy with arms, ammunition, supplies, money, or other thing; or

(2) without proper authority, knowingly harbors or protects or gives intelligence to or communicates or corresponds with or holds any intercourse with the enemy, either directly or indirectly; shall suffer death or such other punishment as a court-martial or military commission may direct.

The Code provision, like the civil law of treason, may be traced for its antecedents to the middle ages. As a matter of fact, Winthrop finds the basis for the substantive provisions of Article 104 in the military code of Gustavus Adolphus in 1621.¹⁷⁷

The equivalent English provisions appeared as Articles 17 and 18 of the British Articles of War of 1765 which were in force at the beginning of the Revolutionary War.¹⁷⁸ These articles were lifted, almost verbatim, into the American Articles of War of

¹⁷⁴ See WINTHROP, *MILITARY LAW AND PRECEDENTS* 629 (2d ed. 1920).

¹⁷⁵ *Ibid.* Winthrop was commenting on the 45th and 46th Articles of War of 1874.

¹⁷⁶ *Id.* at 629-30.

¹⁷⁷ WINTHROP, *op. cit. supra* note 174, at 907. Specifically, see Articles 67-72, 76, 77. The offense antedates even that; see, for example, the trial of Marshall D'Audreham in 1367, noted in Keen, *Treason Trials Under the Law of Arms*, 112 *ROYAL HIST. SOC. TRANS.* 15th 100 (1961).

¹⁷⁸ WINTHROP, *op. cit. supra* note 174, at 931.

1775,¹⁷⁹ and in substance describe the offense contemplated by Article 104.¹⁸⁰

Only one minor variation seems worth noting. The original provision punishing aiding the enemy limited such assistance to "money, victuals, or ammunition,"¹⁸¹ and the language remained unchanged in Article 45 of the 1874 Articles of War.¹⁸² But times had changed. The day where aiding the enemy was limited by the very nature of warfare itself was over. The Civil War had pointed out a myriad of new ways to aid enemies. Winthrop, aware of the undue restriction, considered the old phraseology to be "bald and imperfect."¹⁸³ He argued that a change was necessary, and suggested the insertion of an additional phrase such as "or other thing" or "otherwise."¹⁸⁴ It may be that the proper approach should not have been to add more words, but rather to subtract a few. The provision could have been reduced simply to "Whosoever relieves the enemy." The difficulty may have been that this result would have placed on the courts the burden of interpreting the meaning of "relieves," and opened the door to the return of the "constructive treasons" long feared by the English.

Congress apparently chose to go along with Winthrop's recommendation. In enacting the Articles of War of 1916, the words "or other thing" were inserted.¹⁸⁵ Perhaps Congress selected the wrong phrase. The added language achieved the purpose of substantially broadening the scope of the offense, but created a problem of semantics in the *Olson* case.¹⁸⁶ Olson had achieved notoriety as an orator in North Korean prison camps. At the behest of his captors he engaged in pro-Communist and anti-American speech-making with the mission of "educating" his fellow prisoners. Prosecuted under Article 104, Olson contended that making a speech was not aiding the enemy with any "thing." In a two to one decision the Board of Review disagreed.¹⁸⁷ Noting that aiding

¹⁷⁹ *Id.* at 953, Articles 27-28.

¹⁸⁰ The Court of Military Appeals has characterized Article 104 as bearing a "striking resemblance" to its 1775 counterpart. See *United States v. Batchelor*, 7 U.S.C.M.A. 354, 368, 22 C.M.R. 144, 158 (1956).

¹⁸¹ WINTHROP, *op. cit.* *supra* note 174, at 953, Article 27.

¹⁸² Act of 22 June 1874, Title XIV, Ch. 5, art. 45, 18 Stat. 233

¹⁸³ WINTHROP, *op. cit.* *supra* note 174, at 631.

¹⁸⁴ *Ibid.*

¹⁸⁵ Act of 29 August 1916, § 3, Article 81; 39 Stat. 619.

¹⁸⁶ *United States v. Olson*, 7 U.S.C.M.A. 460, 22 C.M.R. 250 (1957).

¹⁸⁷ CM 384483 Olson, 20 C.M.R. 461 (1956), *aff'd*, 7 U.S.C.M.A. 460, 22 C.M.R. 250 (1957).

30 MILITARY LAW REVIEW

the enemy by participating in propaganda radio broadcasts had been sufficient to predicate at least three civil convictions for treason,¹⁸⁸ the Board of Review concluded that the psychological aspects of warfare had "become as important as arms, ammunition, and guided missiles."¹⁸⁹ The Court of Military Appeals viewed it otherwise. Tracing the history of Article 104, the court concluded that the word "thing" must be equated to "tangible object."¹⁹⁰ Olson's conviction, however, was sustained on the ground that the specification still described the Article 104 offense of communicating, corresponding or holding any intercourse with the enemy.¹⁹¹ The military construction concerning the use of the words "or other thing" is important as the only area where military rule is different from the civil rules applicable to treason by aiding the enemy.

It has been suggested that Article 104 defines a military law of treason. The objections to that are many. Where in Article 104 is any requirement that a conviction must be based on the testimony of two witnesses to the same overt act? Forgetting, for the moment, the crime of treason by levying war, where in the treason statute is aiding the enemy limited to "arms, ammunition, supplies, money, or other thing"? If the two offenses are truly different, in what respects are they different?

An arguable distinction advanced by Winthrop between the offenses described by Article 104 and treason is that the latter is a specific intent offense; that is, there must be proof of an intent to betray.¹⁹² But this view is not uncontested. Dean Miller of Duke University takes a contrary approach. He states: "In order that the crime of treason be committed there must be an intent. However no specific intent is required. It is sufficient that the defendant intended to do the prohibited act."¹⁹³ It is well settled that the offenses described by Article 104 require only a general intent.¹⁹⁴

The problem of intent in treason *cis-ci-cis* Article 104, is one with which the courts have wrestled with only limited success.

¹⁸⁸ 20 C.M.R. at 464.

¹⁸⁹ *Id.* at 463.

¹⁹⁰ United States v. Olson, 7 U.S.C.M.A. 460, 467, 22 C.M.R. 250, 257 (1957).

¹⁹¹ *Id.* at 468, 22 C.M.R. at 258.

¹⁹² See WINTHROP, *op. cit. supra* note 174, at 630.

¹⁹³ MILLER, CRIMINAL LAW 502 (1934).

¹⁹⁴ See MANUAL FOR COURTS-MARTIAL, UNITED STATES, 1951, para. 183; United States v. Batchelor, 7 U.S.C.M.A. 354, 22 C.M.R. 144 (1956).

The problem was squarely raised in the case of *Martin v. Young*, a *habeas corpus* proceeding involving the application of Article 3a, *Uniform Code of Military Justice*, to a serviceman who had been discharged and reenlisted subsequent to alleged Article 104 offenses.¹⁹⁵ This provision permitted court-martial for an offense committed in a previous enlistment, which would otherwise have been prohibited, where the offense was punishable by confinement for five years or more and could not be tried in any United States court.¹⁹⁶ The Government contended that Martin met this criteria and proceeded to charge him under Article 104 for offenses committed in a previous enlistment while a prisoner of war in Korea. The Government's argument was almost contemptuously brushed aside by the court. The conduct alleged against Martin, held the court, would also, *inter alia*, constitute treason and hence he was subject to prosecution in United States courts under civilian federal law.¹⁹⁷ In dealing with the argument that treason was a specific intent offense while Article 104 was not, the court hedged. Looking to the specification itself the court found Martin charged with giving aid to the enemy "wrongfully, unlawfully, and knowingly."¹⁹⁸ This, the court held, imports "criminality" and it was unnecessary to determine whether or not Article 104 denounced a general intent offense.¹⁹⁹ Just what the court meant by "criminality" was never made clear.

The meaning of the holding in the *Martin* case was subsequently discussed by the Court of Military Appeals in the *Batchelor* decision.²⁰⁰ The court referred without comment to Winthrop's conclusion that treason required specific intent and went on to hold that Article 104 required only general intent.²⁰¹ Discussing the case of *Martin v. Young* the court found nothing inconsistent with that holding. It concluded: "What the judge did not say is that Article 104 requires a specific intent, or that it prescribes the offense of treason, or that the Government is prohibited from overproving its case in prosecutions under Article 104."²⁰² Concerned with the intent required under Article 104, the Court of Military Appeals can be accused of looking at *Martin v. Young*

¹⁹⁵ *Martin v. Young*, 134 F.Supp. 204 (N.D. Cal. 1955).

¹⁹⁶ *UNIFORM CODE OF MILITARY JUSTICE*, Article 3a.

¹⁹⁷ 18 U.S.C. § 2381 (1958). See *Martin v. Young*, 134 F.Supp. 204, 207 (N.D. Cal. 1955).

¹⁹⁸ *Id.* at 208.

¹⁹⁹ See *id.* at 208.

²⁰⁰ *United States v. Batchelor*, 7 U.S.C.M.A. 354, 22 C.M.R. 144 (1956).

²⁰¹ *Id.* at 368, 22 C.M.R. at 158.

²⁰² *Ibid.*

30 MILITARY LAW REVIEW

through military justice glasses. It is suggested that the language in that case may well be read, not for the proposition that Article 104 requires specific intent, but that treason requires something less.

Support for this interpretation may be bolstered by a close look at the language found in the Supreme Court opinion in the *Cramer* case.²⁰³ Since intent must be inferred from conduct of some sort, the court concluded it would be permissible to draw the usual reasonable inferences as to intent from the overt acts.²⁰⁴ This language indicates that something less than proof of specific intent will suffice.

The analogy of Article 104 to treason was considered tangentially in the *Dickenson* case.²⁰⁵ The accused there contended that Article 104 was unconstitutional. The court saw the thrust of his contention as implying that the article represents only a particularization of different overt acts of treason.²⁰⁶ When viewed more closely it appears the contention was actually broader; that by applying Article 104 to "any person," and thus including persons not otherwise subject to the Code, Congress was purporting to extend the definition of treason. This would be specifically prohibited by the Constitution. The obvious path to avoid this prohibition would have been for the court to hold that Article 104 and treason were two separate offenses. This the court declined to do, preferring not to reach such a "broad problem."²⁰⁷ Realizing that this approach did nothing to solve the problem, the court rationalized further that since *Dickenson* was clearly a person subject to the Code, he had no standing to try to "vindicate the Constitutional rights" of some third party.²⁰⁸

The close relationship of Article 104 to treason is bolstered by an examination of some of the rules of law applied by the Court of Military Appeals. When faced with problems concerning the substantive law to be applied under Article 104, the court has turned to the civil treason cases. Thus instructions by a law officer which were identical to those approved by Federal courts as stating the law of the affirmative defense of duress to treason

²⁰³ *Cramer v. United States*, 325 U.S. 1 (1944).

²⁰⁴ See *id.* at 31.

²⁰⁵ *United States v. Dickenson*, 6 U.S.C.M.A. 438, 20 C.M.R. 154 (1955).

²⁰⁶ *Id.* at 448, 22 C.M.R. at 164.

²⁰⁷ See *ibid.*

²⁰⁸ See *ibid.*

have been upheld in three cases.²⁰⁹ The civilian rule concerning the lack of motive as an excuse for treason has been applied to Article 104.²¹⁰ The definition of "enemy" has been lifted from its civilian counterpart.²¹¹ The convictions of the "radio traitors" of World War II have been applied for the proposition that the obligations of citizenship continue to rest on the shoulders of one inside a foreign country and subject to the local rules of the enemy.²¹² Indeed, while not required for an Article 104 conviction, the Army has shown itself not unmindful of the two witnesses rule.²¹³ Conversely, the civilian courts have not hesitated to prosecute for treason individuals who, by reason of a break in service, were lost to military jurisdiction.²¹⁴

The usefulness of Article 104 is difficult to gauge. Records of military courts are woefully inadequate to permit research on the extent of its historical application. It is thus impossible to compile any statistics concerning the number of individuals who have been tried and convicted by military courts prior to the enactment of the Uniform Code. Only two cases involving World War II prosecutions in violation of Article of War 81 ever reached the Board of Review level and both involved offenses committed within the United States.²¹⁵ Following the Korean War the offense achieved some vitality as a vehicle for bringing prisoner of war collaborators to trial. It is reported that ten of these individuals were charged under Article 104 and eight convicted.²¹⁶ But its comparative lack of use in no way imports obsolescence. In an age where increased psychological and sophisticated pressures may mold the minds of some to ignore their obligations of loyalty

²⁰⁹ See *United States v. Olson*, 7 U.S.C.M.A. 460, 22 C.M.R. 250 (1957); *United States v. Fleming*, 7 U.S.C.M.A. 543, 23 C.M.R. 7 (1957), CM 388546, Bayes, 22 C.M.R. 487 (1956), *petition for review denied*, 7 U.S.C.M.A. 798, 23 C.M.R. 421, (1957).

²¹⁰ See *United States v. Batchelor*, 7 U.S.C.M.A. 354, 22 C.M.R. 144 (1956).

²¹¹ See *United States v. Dickenson*, 6 U.S.C.M.A. 438, 20 C.M.R. 154 (1955).

²¹² See *United States v. Olson*, 7 U.S.C.M.A. 460, 22 C.M.R. 250 (1957).

²¹³ See U.S. DEPT OF ARMY, FIELD MANUAL 19-5, CIVIL DISTURBANCES AND DISASTERS para. 162b (1958).

²¹⁴ See *United States v. Monti*, 100 F.Supp. 209 (E.D.N.Y. 1951); *United States v. Provoo*, 125 F.Supp. 185 (S.D.N.Y. 1954), *rev'd*, 215 F.2d 531 (2d Cir. 1954), *2d indictment dismissed*, 17 F.R.D. 183 (D. Md. 1955), *aff'd per curiam*, 350 U.S. 857 (1955).

²¹⁵ CM 310327, Leonhard, 61 B.R. 233 (1946); CM 260393, Kissman (B.R., 24 Aug. 1944).

²¹⁶ Note, *Misconduct in the Prison Camp*, 56 COLUM. L. REV. 709, 745-46 (1956).

30 MILITARY LAW REVIEW

to their country, a military law of treason continues to be necessary to provide effective deterrent and adequate punishment.

VII. SUMMARY

A survey of the law of treason leaves little room for conclusions. It is, indeed, a history lesson in which, contrary to Orwell, the past controls the present. At the outset, it can certainly be observed that the current law, both as enacted by statute and interpreted by the courts is heavily dependent on its English antecedents. In every area the law has been found to have derived from its precedents and twentieth century judges have continued to rely on opinions expressed by their ancestors, often hundreds of years ago.

The English law of treason was found to have enjoyed wide and strict application and to have resulted in perhaps thousands of executions. In this area the United States courts have failed to keep pace. While castigating treason as the highest of crimes, the American courts have displayed more concern for individual rights and less for governmental vengeance. In contrast with the English experience, not one man has ever been executed for committing treason against the United States.²¹⁷

Similar generalizations may be made with respect to Article 104, the military law of treason. Colonel Winthrop to the contrary, it appears impractical to call that offense by any other name. While certain legal distinctions may be found between the two offenses they are more than outweighed by the similarities. If the military law is narrower in scope than its civilian counterpart, it is because history has shown no need for a wider application. As a result any number of treasonable acts may be envisaged which would not violate the conduct denounced by Article 104. A prime example would be organized resistance to the enforcement of a federal statute or court order. But not a single instance may be conceived where the act that violates Article 104 would not also constitute treason.

There have been no trials for treason in this country for perhaps fifteen years. It may be partially for this reason that many writers, such as Dame Rebecca West, suggest that treason has entered an area of obsolescence and is passing rapidly to the obsolete. In a time of "cold war" as we know it today, there seems

²¹⁷ John Brown was executed for treason committed against the State of Virginia. See note 54 *supra* and text accompanying.

TREASON

little chance that treason can legally be committed. However a host of related offenses, such as espionage, sedition, advocating the overthrow of the Government, and failing to register as a subversive organization, appear adequate to fulfill the security needs of the state during such a period. But this fact alone does not compel the conclusion that the law of treason has no place in modern society. Today treachery and disloyalty are a more real and serious fear than ever before. The peacetime traitor should, by whatever law is necessary, be penalized for the evil of his works and the wartime traitor punished for the villain that he is.

\mathbf{y}_0

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

**Government Targeted Brief
On Receipt of Intelligence
as a Requirement of
Aiding the Enemy
Enclosure 5**

29 March 2013

Encl 5 to
APPELLATE EXHIBIT 510
PAGE REFERENCED: _____
PAGE OF PAGES

**MANUAL
FOR
COURTS-MARTIAL
UNITED STATES
1951**

Effective 31 May 1951

d. ENGAGING IN LOOTING OR PILLAGING

Discussion.—The words “looting or pillaging” mean unlawfully seizing or appropriating property which is located in enemy or occupied (friendly or enemy) territory and is either left behind or is owned by, or in the custody of, the enemy or occupied state, its inhabitants, or persons who are under its protection or who, immediately before the place where the act occurred had been occupied, were under the protection of the enemy or occupied state. The unauthorized removal or appropriation of any part of the equipment of a seized or captured vessel or the unlawful seizure or appropriation of property owned by or in the custody of the officers, crew, or passengers on board a seized or captured vessel, constitutes the offense of looting or pillaging wherever the vessel may be located at the time of the offense.

Proof.—(a) That the accused unlawfully seized or appropriated certain property; (b) that the property was located in enemy or occupied territory, or that it was on board a seized or captured vessel; and (c) that the property was left behind—or that it was owned by, or in the custody of, the enemy or occupied state or a person having a certain status with respect to the enemy or occupied state, or that it was part of the equipment of a seized or captured vessel, or was owned by, or in the custody of the officers, crew, or passengers on board a seized or captured vessel, as alleged.

183. ARTICLE 104—AIDING THE ENEMY

This article denounces offenses by all persons whether or not otherwise subject to military law. The trial of offenders may be by court-martial or by military commission.

a. AIDING OR ATTEMPTING TO AID THE ENEMY

Discussion.—“Enemy” imports citizens as well as members of military organizations and does not restrict itself to the enemy government or its armed forces. All the citizens of one belligerent are enemies of the government and of all the citizens of the other.

It is not a violation of this article, however, to furnish to prisoners of war subsistence, quarters, and other comforts or aid to which they are lawfully entitled.

To aid the enemy as used in this article is equivalent to furnishing it with the arms, ammunition, supplies, money, or other things as denounced in the article. It is immaterial whether the articles furnished are needed by the enemy or whether the transaction is a donation or sale.

Proof.—That the accused either directly or indirectly aided or attempted to aid the enemy with certain arms, ammunition, supplies, money, or other thing, as alleged.

b. HARBORING OR PROTECTING THE ENEMY

Discussion.—See 183a. An enemy is harbored or protected when, without proper authority, he is shielded, either physically or by use of any artifice, aid, or representation, from any injury or misfortune which in the chance of war may befall him. It must appear that the offense is knowingly committed, but circumstances sufficient to put a reasonable man on notice will be sufficient to charge the accused with notice.

Proof.—(a) That the accused, without proper authority, harbored or protected a certain person; (b) that the person so protected was an enemy; and (c) that the accused had notice or was chargeable with notice of that fact.

c. GIVING INTELLIGENCE TO THE ENEMY

Discussion.—See 183a. This is a particular case of corresponding with the enemy, rendered more heinous by the fact that the communication contains intelligence that may be useful to the enemy for any of the many reasons that make information valuable to belligerents. As in the preceding case, knowledge must be proved, and it is immaterial to the issue of guilt whether the intelligence was conveyed by direct or indirect means. The word "intelligence" imports that the information conveyed is true or implies the truth, at least in part.

Proof.—(a) That the accused, without proper authority, knowingly conveyed to the enemy certain information, as alleged; and (b) that the information was true or implied the truth, at least in part.

d. COMMUNICATING, CORRESPONDING, OR HOLDING INTERCOURSE WITH THE ENEMY

Discussion.—Communication, correspondence, or holding intercourse with the enemy does not necessarily import a mutual exchange of communication. The law requires absolute nonintercourse, and any unauthorized communication, no matter what may be its tenor or intent, is here denounced. The prohibition lies against any method of intercourse or communication whatsoever, and the offense is complete the moment the communication issues from the accused, whether it reaches its destination or not. The words "directly or indirectly" apply to this offense. It is essential to prove that the offense was knowingly committed.

Citizens of neutral powers resident in or visiting invaded or occupied territory can claim no immunity from the customary laws of war relating to communication with the enemy.

Proof.—(a) That the accused, without proper authority, communicated, corresponded, or held intercourse with a certain person; (b) that such person was an enemy; and (c) that the accused had notice or was chargeable with notice of this fact.

))))))))))

)
)
)

)
)
)
)
)

[illegible]

))

U.S. Army. Judge Advocate Gen.

A DIGEST

OF

OPINIONS

OF THE

JUDGE ADVOCATE GENERAL OF THE ARMY,

WITH NOTES,

BY

BVT. COLONEL W. WINTHROP,

Judge Advocate, U. S. Army,

ASSISTANT TO THE JUDGE ADVOCATE GENERAL.

[PUBLISHED BY THE AUTHORITY OF THE SECRETARY OF WAR.]

WASHINGTON:
GOVERNMENT PRINTING OFFICE.
SEPTEMBER 1, 1880.

SECOND THOUSAND.

PREFACE.

The opinions, of which abstracts are presented in this work, consist of a selection from a mass of opinions recorded in the forty four volumes of the Reports of the Bureau of Military Justice, and furnished—mainly to the Secretary of War—by BYT. MAJ. GEN. JOSEPH HOLT, Judge Advocate General, from September, 1862, to December, 1875, and by BRIG. GEN. WM. MCKEE DUNN, Judge Advocate General, from the latter date to the present time. These opinions embrace those given by the Judge Advocate General in the course of his official reviews of the proceedings of military courts, or otherwise in connection with the subject of the administration of justice in the Army; as also those rendered by him in his *ex officio* capacity of general legal adviser to the Secretary of War or law officer of the War Department, upon questions of law arising in the business of that Department, and referred to him for opinion by its Head.

The present work is not properly a later edition of the Digest of which the last issue was published in 1868, but is intended quite to supersede that publication. All that was deemed of permanent value therein has indeed been retained, but much the greater portion of the present volume consists of matter entirely new, or in part new and newly presented. Where practicable, such an arrangement has been made of the extracts as to divest them in a degree of the effect of the *disjecta membra* and give them connection and sequence. With the view of adding to the interest as well as value of the work, the text has been illustrated by notes; the authorities cited being taken from compilations commenced, for personal use, some fifteen years ago, and kept up with the new adjudications, orders, enactments, &c., as they appeared. The references—especially those made to cases in General Orders—might have been considerably extended, but it has been preferred to select such as were especially

pointed and pertinent. The citations include cases reported in 10 Otto, (100 U. S.,) the last volume of the Reports of the Supreme Court, (published in August;) as also cases in the 15th volume of the Reports of the Court of Claims, yet to be published; as well as opinions to be contained in the forthcoming volumes—XV and XVI—of the Opinions of the Attorneys General;* together with General Orders of the series of 1880, as thus far issued from the Headquarters of the Army and of the different military departments.

Except in two or three instances specially indicated, no opinion has been presented in this volume which is known or believed to have been disapproved by the Secretary of War. It is by his authority that the work has not only been printed at the public expense, but, in order that all proper persons desiring the same may be supplied with copies, has also been stereotyped.

* I desire to express my acknowledgments to the Attorney General, Hon. Charles Devens, for his courtesy in permitting me to examine and make extracts from the original opinions as recorded in the Department of Justice. W. W.

that the money, &c., furnished is *exchanged* for some commodity, as cotton, valuable to the other party. XII, 385; XIV, 266; XVI, 446.

4. The act of "relieving the enemy" contemplated by this Article is distinguished from that of trading with the enemy in violation of the laws of war; the former being restricted to certain particular forms of relief, while the latter includes every kind of commercial intercourse not expressly authorized by the government. XIV, 266. [See LAW OF WAR, § 1.]

FORTY-SIXTH ARTICLE.

"Whosoever holds correspondence with, or gives intelligence to, the enemy, either directly or indirectly, shall suffer death, or such other punishment as a court-martial may direct."

1. Held that the offence of *holding correspondence* with the enemy was completed by writing and putting in progress a letter to an inhabitant of an insurrectionary State during the late war; it not being deemed essential to this offence that the letter should reach its destination.¹ IV, 368; V, 274, 287; X, 567.

2. It is essential, however, to the offence of *giving intelligence* to the enemy that material information should actually be communicated to him; the communication may be verbal, in writing, or by signals. XIV, 273.

FORTY-SEVENTH ARTICLE.

"Any officer or soldier who, having received pay, or having been duly enlisted in the service of the United States, deserts the same, shall, in time of war, suffer death, or such other punishment as a court-martial may direct; and in time of peace, any punishment, excepting death, which a court-martial may direct."

SEE DESERTION.

FORTY-EIGHTH ARTICLE.

"Every soldier who deserts the service of the United States shall be liable to serve for such period as shall, with the time he may have served previous to his desertion, amount to the full term of his enlistment; and such soldier shall be tried by a court-martial and punished, although the term of his enlistment may have elapsed previous to his being apprehended and tried."

1. The liability, to make good to the United States the time lost by desertion, enjoined by the first clause of this Article,

¹Compare Hensey's Case, 1 Burrow, 642; Stone's Case, 6 Term, 527; Samuel, 580.

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

)
)
)
)
)
)
)
)
)
)

Government Targeted Brief
On Receipt of Intelligence
as a Requirement of
Aiding the Enemy

Enclosure 7

29 March 2013

Encl 7 to
APPELLATE EXHIBIT 510
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

J. H. Langham
KF
7014
031
1

A TREATISE
ON THE
MILITARY LAW
OF THE
UNITED STATES.

TOGETHER WITH THE
PRACTICE AND PROCEDURE OF COURTS-
MARTIAL AND OTHER MILITARY
TRIBUNALS.

BY
BRIGADIER-GENERAL GEORGE B. DAVIS,
JUDGE-ADVOCATE GENERAL, U. S. A.,
*Formerly Professor of Law at the United States Military Academy,
West Point, New York.*

SECOND EDITION, REVISED
THIRD THOUSAND.

NEW YORK :
JOHN WILEY & SONS.
LONDON : CHAPMAN & HALL, LIMITED.
1911.

that is, to the officers and non-commissioned officers of the guard, to such members of the guard as are actually engaged in the performance of duty as sentinels, and to such other persons as are permitted or required, on account of their official duties, to pass and repass a line of sentinels at night.

The parole, which serves as a check upon the countersign, is given only to those who, by their office or duty, are entitled to visit and inspect guards or sentinels at night. It is used solely as a means of identification, but it cannot avail as a passport unless accompanied by the countersign. The term "watchword," as used in the Article, comprehends not only the countersign and parole, but any preconcerted word or signal issued, by competent authority, for a similar purpose in the performance of guard or outpost duty.

The offense may be committed by any military person who makes known the watchword to one not entitled to receive it, in accordance with existing orders and regulations, or who gives a parole or watchword different from that which he received. As no specific intent is set forth in the statute, the offense may be committed through negligence or inadvertence, or with the intent to convey the watchword to the enemy; the offense would be complete in either case.

ARTICLE 45. *Whosoever relieves the enemy with money, victuals, or ammunition, or knowingly harbors or protects an enemy, shall suffer death, or such other punishment as a court-martial may direct.*

ARTICLE 46. *Whosoever holds correspondence with or gives intelligence to the enemy, either directly or indirectly, shall suffer death, or such other punishment as a court-martial may direct.*

These provisions appear respectively as Articles 18 and 19, Section 14, of the British Code of 1774, as Articles 18 and 19, Section 13, of the American Articles of 1776, and as Nos. 56 and 57 of the Articles of 1806.

In view of the general term of description "whosoever" in these Articles it was held, during the late war, by the Judge-Advocate-General and by the Secretary of War, and has been held later by the Attorney-General, that civilians, equally with military persons, were amenable to trial and punishment by court-martial under either Article.¹ But the sounder construction would seem to be that, as the Articles of War are a code enacted for the government of the military establishment, they relate only to persons belonging to that establishment unless a different intent should be expressed or otherwise made manifest. No such intent is so expressed or made manifest. Persons not belonging to the military establishment may be proceeded

¹ Dig. J. A. Gen., 40, par. 1. Admitting this construction to be warranted so far as relates to acts committed on the theatre of war or within a district under martial law, it is to be noted that it is the effect of the leading adjudged cases to preclude the exercise of the military jurisdiction over this class of offenses when committed by civilians in places not under military government or martial law. See, especially, *Ex parte Milligan*, 4 Wallace, 121-123; *Jones vs. Seward*, 40 Barb., 563. *Ibid.*, 40, par. 1, note.

against for the acts mentioned in the Article, but it is by virtue of the power of another jurisdiction, namely, martial law; and martial law does not owe its existence to legislation, but to necessity.¹ The scope of these Articles under the legislation of 1776, apparently extending their application to civilians, seems to have been modified as a consequence of the adoption of the Constitution.

Relieving the Enemy.—The act of "relieving the enemy" contemplated by this Article is distinguished from that of trading with the enemy in violation of the laws of war; the former being restricted to certain particular forms of relief, while the latter includes every kind of commercial intercourse not expressly authorized by the government.² It is none the less relieving the enemy under this Article that the money, etc., furnished is exchanged for some commodity, as cotton, valuable to the other party.³

Holding Correspondence with the Enemy.—The offense of holding correspondence with the enemy is completed by writing and putting in progress a letter to an enemy, as to an inhabitant of an insurrectionary State during the late war; it not being deemed essential to this offense that the letter should reach its destination.⁴ It is essential, however, to the offense of giving intelligence to the enemy that material information should actually be communicated to him; and such communication may be verbal, in writing, or by signals.⁵

"The rule which declares that war makes all the citizens or subjects of one belligerent enemies of the government and of all the citizens or subjects of the other applies equally to civil and to international wars." An insurrectionary State is no less "enemy's country," though in the military occupation of the United States, with a military governor appointed by the President.⁶

ARTICLE 47. *Any officer or soldier who, having received pay or having been duly enlisted in the service of the United States, deserts the same, shall, in time of war, suffer death, or such other punishment as a court-martial may direct; and in time of peace, any punishment excepting death which a court-martial may direct.*

The first statutory recognition of this offense in England dates from the middle of the fifteenth century, and will be found in an enactment⁷ conferring the status of felony upon a soldier who deserted from the captain whom

¹ Opin. J. A. Gen.

² Dig. J. A. Gen., 41, par. 4.

³ *Ibid.*, par. 3.

⁴ *Ibid.*, 42, par. 1.

⁵ *Ibid.*, par. 2.

⁶ The Service, 2 Wall., 274, 418. See, also, the opinion of the U. S. Supreme Court (frequently since reiterated in substance) as given by Grier, J. in the "Prize Cases," 2 Black, 666 (863), and by Chase, C.J., in the cases of *Mrs. Alexander's Cotton*, and *Dig. J. A. Gen.*, 41, par. 2.

⁷ 18 Henry VI., ch. 19.

γ_1

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Government Targeted Brief
On Receipt of Intelligence
as a Requirement of
Aiding the Enemy
Enclosure 8

29 March 2013

Encl 8 to
APPELLATE EXHIBIT 510
PAGE REFERENCED: _____
PAGE _____ OF _____ PAGES

WAR DEPARTMENT
OFFICE OF THE JUDGE ADVOCATE GENERAL

Army

U. S. Judge-advocate general's

2 A DIGEST OF OPINIONS

OF THE

JUDGE ADVOCATES GENERAL
OF THE ARMY

1912



WASHINGTON
GOVERNMENT PRINTING OFFICE
1917

355
Un 332d
1912
corp. 2.

WAR DEPARTMENT,
OFFICE OF THE CHIEF OF STAFF,
Washington, February 17, 1912.

The following Digest of Opinions of the Judge Advocates General of the Army, prepared under the direction of the Judge Advocate General, United States Army, by Capt. Charles Roscoe Howland, Twenty-first Infantry, Assistant to the Judge Advocate General, is published for the information of the Army and Organized Militia of the United States.

By order of the Secretary of War:

LEONARD WOOD,
Major General, Chief of Staff.

XLV B. During the War of the Rebellion all inhabitants of insurrectionary States were *prima facie* enemies in the sense of this and the succeeding article.¹ *R. 14, 266, Mar., 1865.* A citizen of an insurgent State who entered the United States military service became of course no longer an enemy. So held of a lieutenant of the First East Tennessee Cavalry. *R. 29, 206, Aug. 1869.*

XLV C. It is no less a *relieving* an enemy under this article that the money, etc., furnished is *exchanged* for some commodity, as cotton, valuable to the other party. *R. 12, 385, Mar., 1865; 14, 266, Mar., 1865; 16, 446, Aug., 1865.*

XLV C 1. The act of "relieving the enemy" contemplated by this article is distinguished from that of trading with the enemy in violation of the laws of war; the former being restricted to certain particular forms of relief, while the latter includes every kind of commercial intercourse not expressly authorized by the Government. *R. 14, 266, Mar., 1865.* (See War.)

XLVI A. Held that the offense of *holding correspondence* with the enemy was completed by writing and putting in progress a letter to an inhabitant of an insurrectionary State during the War of the Rebellion; it not being deemed essential to this offense that the letter should reach its destination.² *R. 4, 370; 5, 274 and 291, Nov., 1863; 10, 567, Nov., 1864.*

XLVI B. It is essential, however, to the offense of *giving intelligence* to the enemy that material information should actually be communicated to him; the communication may be verbal, in writing, or by signals. *R. 14, 273, Mar., 1865.*

XLVIII A. Held that when a deserter is returned to duty without trial there is an implied admission on his part of the desertion. This admission establishes the desertion and entails the requirement in the forty-eighth article of war that he shall make good the time lost in desertion.³ *R. 63, 276, Apr., 1887, P. 26, 487, Sept., 1888; C. 18306, Apr. 11, 1908; 16314, Sept. 5, 1904 and Nov. 13, 1906; 20690, Nov. 23, 1906; 21117, Feb. 15, 1907.*

were made manifest. No such intent is so expressed or made manifest. Persons not belonging to the military establishment may be proceeded against for the acts mentioned in the article, but it is by virtue of the power of another jurisdiction, namely, martial law; and martial law does not owe its existence to legislation but to necessity. The scope of these articles under the legislation of 1776, apparently extending their application to civilians, seems to have become modified on the adoption of the Constitution.

Possibly the sixty-third article of war should be construed as making "retainers to the camp," etc., part of the military forces for the time being. But see the case of B. G. Harris, M. C., tried by court-martial in 1865. (H. Ex. Doc. 14, 39th Cong., 1st sess.)

¹ See the opinion of the United States Supreme Court (frequently since reiterated, in substance, as given by Grier, J., in the "Prize Cases," 2 Black, 635, 666 (1862); and by Chase, C. J., in the cases of Mrs. Alexander's Cotton, and The Venice, 2 Wallace, 238, 274, 418 (1864). In the latter case the Chief Justice observes: "The rule which declares that war makes all the citizens or subjects of one belligerent enemies of the Government and of all the citizens or subjects of the other, applies equally to civil and to international wars." That an insurrectionary State was no less "enemy's country," though in the military occupation of the United States, with a military government appointed by the President. (See Opinion by Field, J., in Coleman v. Tennessee, 7 Otto, 509, 518, 517.)

² O'Brien, 147; Hensley's Case, 1 Burrow, 642; Stone's Case, 6 Term, 527; Samuel, 580.

³ 26 Op. Atty. Gen., 239.

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

**Government Targeted Brief
on Courtroom Closures**

29 March 2013

On 1 March 2013, the United States offered to submit a targeted brief on courtroom closures in the military and federal systems, to include analyses on whether recent case law relating to the right to a public trial affects the requirements under *United States v. Grunden*, 2 M.J. 116 (C.M.A. 1977), and to what extent military and federal courts have closed proceedings.

In the first section of this targeted brief, the United States explains whether recent case law relating to the right to a public trial affects the requirements under *Grunden*. Case law is clear that the requirements of *Grunden* still apply, yet must be read in concert with Rule for Courts-Martial (RCM) 806.

In the second section of this targeted brief, the United States explains the details underpinning various courtroom closures, particularly upon what courts have relied to close the courtroom, to what extent the courts have closed the courtroom, and what, if any, measures the Court may adopt, both during and after court closure, to further control that which is closed to the public. Ultimately, government counsel in military and federal cases have employed various methods, based on the facts of the case and nature of the materials in question, to demonstrate the classified nature of the material and to identify those portions of its case which will involve this material to justify courtroom closure, consistent with the balancing test under RCM 806.

FACTS

On 31 January 2013, the United States requested courtroom closure, in whole or in part, for the testimony of 37 of the 141 government witnesses and provided the particular subject matter to which each witness would testify in a closed session. See Appellate Exhibit (AE) 479. The United States estimated that the requested closures comprised approximately 30% of its case.

On 1 March 2013, the Court ordered the United States to provide more specificity with respect to which portions of testimony closure was sought. See AE 503. In its supplemental response, the United States provided a greater degree of specificity. See AE 505. Further, in light of reasonable alternatives available short of closure, the United States narrowed its list of witnesses for whose testimony closure was sought to 28. The United States currently estimates that the requested closures compromise approximately 25% of its case. See *id.*

APPELLATE EXHIBIT 511
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

WITNESSES/EVIDENCE

The United States requests the Court consider the enclosures to this filing and the Appellate Exhibits cited herein.

DISCUSSION

I. *Grunden* is Still Good Law Yet Must be Read in Concert with RCM 806

The right to a public trial derives from two sources: first, the Sixth Amendment, in so far as it attaches to the accused, *see* Manual for Courts-Martial, United States, R.C.M. 806(a) analysis, at A21-48 (2012); *see also* *Waller v. Georgia*, 467 U.S. 39, 46 (1984); and second, the First Amendment, in so far as it applies to the public, *see* RCM 806(a) analysis, at A21-48; *see also* *Richmond Newspapers, Inc., et al. v. Virginia et al.*, 448 U.S. 555, 580 (1980). The right to a public trial is not absolute. *See* *ABC Inc. v. Powell*, 47 M.J. 363, 365 (C.A.A.F. 1997). Both the military and federal systems adopt a balancing test to curtail this right. *See* RCM 806(b)(2); *see also* *Press-Enterprise Co. v. Superior Ct. of California*, 464 U.S. 501, 509 (1984); *Waller*, 467 U.S. at 48.

In the military system, the seminal case on courtroom closures remains *Grunden*. *See* *Denver Post Corp. v. United States*, 2005 WL 6519929, at 2 (A.C.C.A. 2005) (encouraging practitioners to apply the “valuable, practicable guidance in the context of excluding the public and press from court-martial trial proceedings” set out in *Grunden*); *see also* *Stars and Stripes v. United States*, 2005 WL 3591156 (N-M. Ct. Crim. App. 2005) (following *Grunden* when addressing issues of potential release of classified information during public court-martial proceedings). The guidance provided in *Grunden* is as follows:

It is our decision that the balancing test employed by a trial judge in instances involving the possible divulgence of classified material should be as follows. His initial task is to determine whether the perceived need urged as grounds for the exclusion of the public is of sufficient magnitude so as to outweigh “the danger of a miscarriage of justice which may attend judicial proceedings carried out in even partial secrecy.” *Stamnicarbon, N.V. v. American Cyanamid Co.*, 506 F.2d 532, 539 (2d Cir. 1974). This may be best achieved by conducting a preliminary hearing which is closed to the public at which time the government must demonstrate that it has met the heavy burden of justifying the imposition of restraints on this constitutional right. The prosecution to meet this heavy burden must demonstrate the classified nature, if any, of the materials in question.

Grunden, 2 M.J. at 121-122. During this initial step, “[a]ll that must be determined is that the material in question has been classified by the proper authorities in accordance with the appropriate regulations.” *Grunden*, 2 M.J. at 122. The Court of Military Appeals (CMA) continued that the trial judge “must further decide the scope of the exclusion of the public”

which will require the prosecution to “delineate which witnesses will testify on classified matters, and what portion of each witness’ testimony will actually be devoted to this area.” *Id.*, at 123. To this day, this process outlined in *Grunden* serves as the backbone underlying the necessary balancing test for courtroom closure. See *Denver Post Corp.*, 2005 WL 6519929, at 2 (encouraging practitioners to apply the *Grunden* guidance).

In *Waller*, 467 U.S. 39, the Supreme Court first articulated this balancing test. To close proceedings and thereby limit the right to a public trial, the trial judge must 1) decide that the party seeking closure has advanced an overriding interest likely to be prejudiced, 2) find that closure is no broader than necessary to protect that interest, 3) consider alternatives to closure, and 4) make findings adequate to support the closure. See *Waller*, 467 U.S. at 48 (adopting the *Press-Enterprise* approach articulating a four-part test for balancing interests at stake in closure). In 2004, RCM 806 was amended to reflect the Supreme Court’s balancing test in light of military case law set forth in *ABC Inc.*, 47 M.J. at 363 and *United States v. Hershey*, 20 M.J. 433, 436 (C.M.A. 1985), which interpreted *Grunden* and applied the Constitutional standard enunciated by the Supreme Court. See RCM 806(b) analysis, at A21-49. And so, *Grunden* is not at odds with the later Supreme Court cases, provided it is read in concert with RCM 806 which imports them to military jurisprudence.

Though both the military and federal systems apply substantively the same balancing test when considering closure, closure to protect classified information is only available in the military system. Military courts follow RCM 806 when closing the courtroom and are explicitly authorized by MRE 505(j) to close proceedings to protect classified information. Cf. *United States v. Anderson*, 46 M.J. 728, 729 (A.C.C.A. 1997) (stating that “absent national security concerns or other adequate justification clearly set forth on the record, trials in the United States military justice system are to be open to the public.”); see also RCM 806(b) analysis, at A21-48 (stating that “the only time trial proceedings may be closed without the consent of the accused is when classified information is to be introduced”). In the federal system, protection of classified information does not amount to the many reasons that federal trial courts may close proceedings. See e.g. *United States v. Zimmerman*, 19 C.M.R. 806, 814 (A.F.B.R. 1955); *Globe Newspaper Co. v. Superior Court for Norfolk County*, 457 U.S. 596 (1982); *United States v. Short*, 41 M.J. 42 (C.M.A. 1994); *United States v. Thunder*, 438 F.3d 866, 868 (8th Cir. 2006); *United States v. Farmer*, 32 F.3d 369 (8th Cir. 1994); *Bobb v. Senkowsk*, 196 F.3d 350 (2nd Cir. 1999); *LaPlante v. Crosby*, 133 Fed. Appx. 723 (11th Cir. 2005). Instead, federal law has procedures in place to protect classified information via the Classified Information Procedures Act (CIPA). See *United States v. Abu Ali*, 528 F.3d 210, 246-49 (4th Cir. 2008); see also *In re Terrorist Bombings of U.S. Embassies in East Africa v. Odeh*, 552 U.S. 93, 120-23 (2nd Cir. 2008); *United States v. Aref*, 533 F.3d 72, 78-81 (2nd Cir. 2008).

II. Extent of Closure

The Rules pursuant to which military courts evaluate closure requests are RCM 806(b)(2) and Military Rule of Evidence (MRE) 505(j). As discussed above and through recent filings, these rules must be read together with *Grunden*. See AE 507. As instructed by the Army Court of Criminal Appeals (ACCA) in *Denver Post Corp.*, *Grunden* can provide focus on how to apply and make the closure decision provided for in RCM 806 and MRE 505(j). Below, the United

States highlights the details underpinning various courtroom closures, focusing particularly on what courts have relied upon to close the courtroom, to what extent the courts have closed the courtroom, and what, if any, measures the Court may adopt, both during and after court closure, to further control that which is closed to the public. The United States has included a more expansive and thorough case-by-case explanation of courtroom closures, both in military and federal courts, in the subsequent section.

A. Demonstration of Need for Closure.

Grunden makes it clear that the Court's "task is to determine whether the perceived need urged as grounds for the exclusion of the public is of sufficient magnitude so as to outweigh 'the danger of a miscarriage of justice which may attend judicial proceedings carried out in even partial secrecy'." *Grunden*, 2 M.J. at 122 (citing *Stamicarbon, N.V. V. American Cyanamid Co.*, 506 F.2d 532, 539 (2d Cir. 1974)). *Grunden* continues that "the prosecution to meet this heavy burden must demonstrate the classified nature, if any, of the materials in question." *Id.* at 122. As the following cases and enclosed material prove, the "method used by the prosecution to satisfy this burden...will vary depending upon the nature of the materials in question and the information offered." *Id.*

In *United States v. Lonetree*, 31 M.J. 849 (N-M. C.M.R. 1990, *aff'd and rem'd*, 35 M.J. 396 (C.M.A. 1992), government counsel met its burden by demonstrating the need for closure during witness testimony consisting of classified information with sworn affidavits which set forth "[a] list of these officers [who will provide testimony on classified matters] and the government's rationale for requesting that they testify in closed session." *Id.*, at 853. The Court interpreted *Grunden* to require "individualized decision-making as to specific information which the Government asserts must be exempted from disclosure at a public trial" – *not* judicial findings for each closed session. See *Lonetree*, 31 M.J. at 854 (emphasis added). Here, the United States submitted its list of witnesses and a detailed description of the testimony for which closure is sought, and the applicable classification guides confirming the classification level of that information. See AE 505. The United States has demonstrated the need for closure under *Lonetree*.

B. Extent of Closure.

Pursuant to *Grunden* and consistent with RCM 806, the prosecution must then justify closure by specifying "which witnesses will testify on the [matter at issue as well as] what portion of each witness' testimony will actually be devoted to this area" and the Court must "decide [on] the scope of the exclusion of the public." *Id.* at 123 (finding that, "even assuming a valid underlying basis for the exclusion of the public, it is error of 'constitutional magnitude' to exclude the public from all of a given witness' testimony when only a portion is devoted to classified material"). This Court must "engage in the necessary analysis as to each witness' expected testimony and to understand in advance how and why it could touch on a classified matter before excluding the public." *Denver Post Corp.*, 2005 WL 6519929, at 3; see also *Grunden*, 2 M.J. at 121-22. To do so, the Court noted that it may "require counsel for both sides to disclose the subjects of their questions for a witness in advance in a closed session." *Denver Post*, 2005 WL 6519929, at 3. On 15 March 2013, the United States did just that by providing

this Court with the detailed subjects of its questions for each witness whose testimony it requests courtroom closure. See AE 505. The United States is aware of no case law requiring more than the subject of that which will be elicited during the closed proceeding to justify closure. The issue, therefore, is to what extent the courtroom may be closed.

Generally, the extent of closure depends entirely upon the facts and circumstances of each case. See *ABC Inc.*, 47 M.J. at 365 ("every case that involves limiting access to the public must be decided on its own merits . . . and the scope of closure . . . tailored to achieve the stated purposes") (referencing *San Antonio Express-News v. Morrow*, 44 M.J. 706, 710 (A.F.C.M.R. 1996) and *Hershey* 20 M.J. at 436); see also *Grunden*, 2 M.J. at 121 (emphasizing the importance of a balancing test employed to examine and analyze the need for and scope of any suggested exclusion). In *United States v. Terry*, 52 M.J. 574 (N.M.C.C.A. 1999), the Court cited *Grunden* saying:

While we did note in *Anzalone* that the closed portion of the trial was limited to 79 pages of the 479-page record of trial, our superior court expressed quite clearly in *Grunden* that "the propriety or impropriety of the exclusion of the public from all or part of a trial cannot, as attempted by the Government in this case, be reduced to solution by mathematical formulas. The logic and rationale governing the exclusion, not mere percentages of the total pages of the record, must be dispositive."

Terry, 52 M.J. at 578 (citing *Grunden*, 2 M.J. at 120 fn 2) (emphasis added). This position is consistent with the Supreme Court's decision in *Globe Newspaper Co.* and numerous federal circuit court cases. See *Globe Newspaper Co.*, 457 U.S. at 605 (finding that the interest supporting the exclusion is what should drive closure inquiry); *In Re Washington Post Co. v. Soussoudisi*, 807 F.2d 383, 392 (4th Cir. 1986) (the trial court is required to execute the closure analysis by evaluating the principles and interests at stake, considering possible alternatives, and articulating findings adequately supporting their closure decision); *Judd v. Haley*, 250 F.3d 1308, 1319 (11th Cir. 2001); *Thunder*, 438 F.3d at 868; *Walton v. Briley*, 361 F.3d 431, 433 (7th Cir. 2004); see also *Ayala v. Speckard*, 131 F.3d 62, 70 (2nd Cir. 1997) (the greater the closure sought, the more "must be the gravity of the required interest and the likelihood of risk to that interest").

For courtroom closures based on the disclosure of classified information, the courts in *Lonetree* and *Denver Post* are again instructive. The Court in *Lonetree* made it clear that the extent of closure for purposes of divulging classified information should be focused on the particular information for which closure is sought. See *Lonetree*, 31 M.J. at 853 (stating that "MRE 505 is directed towards the information sought to be exempted from disclosure at public trial" and thus when "the information may be divulged by a number of witnesses or documents, or both, the focus of exclusion is upon that specific information"). The Court explained that "the specificity required [in the military judge's decision] addresses the information to be protected, not through what method it is disclosed." *Id.* Here, as in *Lonetree*, the scope of exclusion should be focused on the specific classified information that may be divulged.

In *Lonetree*, the appellate court applauded the extent of closure employed as “the fairest and most practical that could be devised” and one that “allowed both parties a reasonably normal context within which to pursue their respective positions.” See *Lonetree*, 31 M.J. at 853. The extent of closure in *Lonetree* was follows:

The extent of the closures was determined by *either* Government or defense. The military judge had already determined which information, because of its classified status, would be presented in closed sessions. The fact that certain unclassified information was disclosed by individuals whose duties and identities could not be publicly matched-up was necessary to protect classified information. Further bifurcation of other witnesses' testimony, other than as occurred, was impracticable and would have created unnecessary chaos.

Lonetree, 31 M.J. at 854. Other military courts also recognize that, in some circumstances, bifurcating testimony may be impractical. In *Denver Post Corp.*, for example, the ACCA contemplated that “in a few instances, the witnesses' testimony could be fairly characterized as so inextricably linked to classified matters as to make it all properly received in a closed session.” *Denver Post Corp.*, 2005 WL 6519929, at 3. The Court agreed that it could be difficult if not impossible to separate the classified information from the unclassified information for several witnesses who dealt directly and solely with the investigative and initial reporting of the events under review. See *id.*

C. Control or Curative Measures.

Even after the public is excluded from the court, the Court has available control or curative measures to further maximize the openness of the proceeding. In *Press Enterprise*, the Supreme Court noted that “[w]hen limited closure is ordered, the constitutional values sought to be protected by holding open proceedings may be satisfied later by making a transcript of the closed proceedings available within a reasonable time, if the judge determines that disclosure can be accomplished while safeguarding the [interest requiring protection].” *Press-Enterprise Co.*, 464 U.S. at 512. This guidance has been echoed by federal cases in numerous circuits. See *Hearst Newspapers v. Cardenas-Guillen*, 641 F.3d 168 (5th Cir. 2011); *Smillie v. Greiner*, 99 Fed. Appx. 324 (2nd Cir. 2004) unpub. Therefore, at trial, should this Court determine that disclosure of some testimony elicited during the closed proceeding is not “necessary to permit a contextual and complete understanding of the classified testimony” and would not jeopardize the protection of classified information, the Court may order an unclassified portion of the transcript of the closed proceeding to be made available. See Enclosure 1. Another possibility under this scenario is for the witness, whose testimony during a portion of the closed proceeding may be disclosed to the public without risking disclosure of classified information, to provide an unclassified summary of those portions of testimony which can be disclosed to the public.

D. Digest of Courtroom Closures.

The below cases and enclosed trial materials may be helpful in understanding what other judges have considered, but also do not articulate clear thresholds. The United States has found no federal authority explaining how much material the Government must put before a Federal trial judge in order to meet *Waller* balancing test requirements. Instead, both military and federal case law suggest that facts and not a particular percentage or a specific asserted interest are controlling.

The below cases are consolidated into the following sections: (1) federal cases closed on the merits but not for classified information; and (2) military cases closed for classified information. In the first section, each paragraph details the extent to which the proceedings were closed as well as why the appellate authority found the closure in constitutional accordance. In the second sections, paragraphs include information on the stage of proceeding closed, the extent of the closure, and information on justification for that closure.

The United States has provided as enclosures abbreviated versions of many of the sources cited because they are not available on Westlaw or LexisNexis. These enclosures will be additionally referenced parenthetically in the respective citations. Additionally, one of the enclosures is provided to the Court *ex parte*. The United States will provide a redacted version of this enclosure to the defense.

i. Federal Case Examples: Closed on Merits but not for Classified Information

Johnson v. Sherry, 586 F.3d 439 (6th Cir. 2009) – Closed for Witness Protection

- **Misconduct and Outcome:** The defendant was convicted of (intent to commit) murder and possession of a firearm during commission of a felony in Michigan state court.
- **Extent of Closure:** At the start of the initial trial, the prosecutor moved to close the courtroom to spectators during the testimony of three prosecution witnesses (two of whom claimed to have seen the shooter). The three individuals were afraid to testify publicly given that two other prosecution witnesses had been killed under suspicious circumstances. The prosecution requested total closure; the defense acquiesced but requested closure not be ordered in presence of jury. The trial court did not remove anyone from the courtroom, but instead instructed in the absence of the defendant's relatives.
- **Justification:** The appellate authority noted the absence of trial court findings to facilitate its decision and expressed concerns about the breadth of the closure ordered – saying, the “prosecution offered no proof that Johnson or any member of Johnson's family was involved in the death of those individuals” and “did not point to any incidents in which the witnesses at issue had been threatened or otherwise contacted by any member of Johnson's family.” (emphasis added) The court also mentioned that the record contained no evidence the defense's failure to object was strategic.

- **Disposition:** The Federal district court granted partial appeal to consider whether the defendant was denied his right to a public trial. After considering the above, the Court ordered an evidentiary hearing “to determine [among other things] whether closure of the trial was justified.”

Smillie v. Greiner, 99 Fed. Appx. 324 (2nd Cir. 2004) unpub. – Closed for the protection of informants and officers

- **Misconduct and Outcome:** Co-defendants (convicted of various crimes) alleged abridgement of their Sixth Amendment right to a public trial.
- **Extent of Closure:** The courtroom was fully closed during the testimony of a confidential informant and an undercover police officer.
- **Justification:** With regards to the confidential information. The court stated the safety of the witness was an “overriding interest” and that the closure occurred solely during the CI’s testimony meant the closure was “no broader than necessary.” Additionally, holding that where neither party suggested alternatives, trial judges are not obliged to consider them *sua sponte*, and so, the alternatives prong was satisfied. And finally, since the trial court’s findings were explicit that there were threats to the informant’s life and family, the findings prong was likewise satisfied. These same reasons applied to the officer. Yet the appellate court expanded its mention of the interests at issue to include protecting his usefulness as an undercover officer. Moreover, the Second Circuit concluded that by making the transcript available to the public and not sealing the courtroom for other law enforcement officers, the trial court demonstrated that it used discretion in closure.
- **Disposition:** The Second Circuit held both closures comported with the requirements of the *Waller* balancing analysis.
- **Note:** *Bowden v. Keane*, 237 F.3d 125 (2nd Cir. 2001), *Bobb v. Senkowski*, 196 F.3d 350 (2nd Cir. 1999), and *Ayala v. Speckard*, 131 F.3d 62 (2nd Cir. 1997) also uphold the trial court’s decision to fully close the courtroom to hear the testimony of an undercover police officer for very similar reasons as *Smilie*.¹ Though earlier than the two cases described above, all three are published.

Application: The above cases are consistent with the proposition that what matters most to appellate courts considering whether the public trial right has been abridged is not a particular interest or amount of closure, but rather that the trial judge has: taken the time to gather the case-specific information, weighed the interests at stake, considered proposed alternatives, and ordered closure targeted only at those interests through findings. In conducting that evaluation, the cases highlight that closure for the entire testimony of a single witness can be “no broader than necessary” if the interest warranting closure attaches to that witness, and that by keeping the

¹ The Federal circuit courts have also approved total closure to protect victims and minor children. These cases are not relayed here because the subject matter differs more from the interests driving the Government’s pursuance of closure in the case at hand. However, information on these courts and their application of the balancing tests used can be provided to the Court should the Court desire.

court open for other witnesses of a similar type that trial court can demonstrate discretion. Finally, the cases highlight that ability to produce a transcript can alleviate some of the public trial concerns. This last proposition is also supported by Supreme Court case *Press-Enterprise* and Fifth Circuit case *Hearst Newspapers v. Cardenas-Guillen*, 641 F.3d 168 (5th Cir. 2011) (hereinafter *Hearst*). The *Hearst* court wrote: “When . . . closure is ordered, the constitutional values sought to be protected by holding open proceedings may be satisfied later by making a transcript of the closed proceedings available within a reasonable time, if the judge determines that disclosure can be accomplished while safeguarding’ the interest that gave rise to the need for closure.” *Hearst* at 181 citing *Press-Enterprise* at 512. In the case of classified information, perhaps any unclassified information which surfaces during the closed testimony could be produced as a redacted transcript as soon as practicable.

ii. Persuasive Military Case Examples: Closure for Classified Information

United States v. Steele, 2011 WL 414992 (A.C.C.A. 2011) unpub.²

- **Misconduct and Outcome:** Defendant pled guilty to and was convicted of wrongfully making and storing classified information in violation of a regulation and possessing pornography in violation of a general order. He was further found guilty of failing to obey a lawful order, conduct unbecoming, and retaining national defense information.
- **Extent of Closure:** According to the record of trial, the case involved seventeen courtroom closures to hear the classified portions of some sixteen of the total forty-two witnesses. These portions include both classified and unclassified material. There were also two additional closures – one for a *Grunden* hearing and one to consider closure under RCM 506 (unclassified Government information).
- **Justification:** While the record does not contain a written closure order or written findings on closure, the Court did have a *Grunden* hearing – a transcript of which is enclosed with this filing. See Enclosure 2.³ In the hearing the Court considered the classified information in three sections – a group of documents already specified as appellate exhibits, a group of redacted documents from which defense requested use of information behind redactions, and a third smaller group of documents having been reviewed later than the others. Notwithstanding the separate groupings, the Court undertook virtually the same inquiry.

The prosecution began by referencing the documents’ classification and the OCA declaration and affidavits related to it. Eventually, the prosecution specified which witnesses it anticipated testifying about those documents. When presenting this information to the court, the Government specified only that the witness would cover

² As courtroom closure issues were not raised on appeal, the citation offered here is provided so the Court may reference background information for and appellate consideration of the case. It is not intended as a citation for the closure employed in the original trial.

³ The Court also had a hearing on closure under 506. As that hearing focused on closure for non-classified information pursuant to a Rule not at issue here, neither is the transcript of any 506 proceeding enclosed nor does the above closure description describe any potential findings on that issue.

how the document related to national defense, how the information could be used to the injury of the United States, and how it related to the elements of the charged offenses. The prosecution did not address what exactly the witness would say. Then, the military judge would announce either the document and general description thereof ("defense plan for X") or the piece of information the defense wanted to use ("information about Y-procedures" or "Z-kind of people") and its classification marking. The judge would mention he had considered the relevant OCA declarations and document markings and was satisfied that 1) the documents were properly classified in accordance with relevant Executive Order provisions and 2) their public disclosure posed reasonable risk of harm or danger to national security interests. After the inquiry about the information in each section, the Judge would ask the trial counsel about the method of its intended expression (testimony). He explained that this inquiry matters so that he can determine how the sessions would flow in the interests of judicial economy and public movement. He specified in most circumstances that the counsel should call a witness, have that witness testify to the greatest extent possible about unclassified matters such as biographical information and then proceed into a classified session. However, the judge recognized that some identity information may itself be classified and therefore warrant greater closure.

During the hearing, the judge also commented that impact witnesses could announce an unclassified general opinion in open court yet discuss specific opinions and the examples on which they are based in closed court. Moreover, he suggested that the findings about harm and classification on which the courtroom closure order is based could be applied to any witness who would testify about classified information addressed not just those witnesses specified during the session.⁴ Finally, he also noted that counsel should construct direct examination questions bearing in mind that classified information should be elicited together so as to minimize the opening and closing of the proceedings.

- **Disposition:** Public trial rights were neither raised by the accused nor addressed by the appellate authority on appeal. Apart from one specification on other grounds, the guilty findings were affirmed.
- **Proposition:** This case is highly instructive for five main reasons. First, the judge indicates that courtroom closure is appropriate wherever the content of the classified document must be discussed. Second, that the judge had to hold a *Grunden* hearing to specify those bits of information the defense wished to use but which otherwise required redactions, highlights the limitation of redactions as an alternative to closure. This is consistent with the Government's discussion of redaction as an alternative in its initial *Grunden* filing. See AE 480. Third, that the judge considered the information first before inquiring about the method of its introduction is consistent with the instruction in *Lonetree* that it is the information and not the method of its delivery which requires specificity. This proposition is further respected by this judge's willingness to decide a topic of information warrants closure and then apply that closure requirement to any witness who may testify about it – only asking the counsel which witnesses will discuss

⁴ This comes from Page 285, Line 18- 286, Line 14 in the classified *ex parte* filing provided to the Court. See Enclosure 3. Other descriptions provided are evidenced primarily in the unclassified portions.

the information in order to establish its relevance and get a projection of proceeding flow. Fourth, the judge recognizes that just because a witness may be able to give an unclassified general opinion of impact, it should not prevent counsel from eliciting a more specific opinion including classified examples during closed session. And finally, the judge mentioned how the counsel should construct a direct examination by grouping all classified information together but never asked them to provide a copy of those questions.

United States v. Anderson, 68 M.J. 378 (C.A.A.F. 2010)⁵

- **Misconduct and Outcome:** The accused was convicted of conduct prejudicial to good order and discipline as well as attempting to give intelligence to the enemy, to communicate with the enemy, and to aid the enemy.
- **Closure:** During the lower court proceedings, the military judge ordered courtroom closure for two witnesses.
- **Justification:** One witness would testify to unclassified but sensitive and not publically disclosed information about weapons systems. The Government sought MRE 506 closure.⁶ The other witness would testify to classified weapons system information.⁷ Before making the closure decision, the judge held an Article 39(a) session for the presentation of evidence and argument. Although the United States is not in possession of the classified record of trial, the closure order reveals that the judge in *Anderson* applied the balancing test after having reviewed the evidence and the relevant classification declaration or privilege assertion with the Court Security Officer. The judge found proper classification and the risk of harm. The conclusions of law mirrored these findings, applying the preponderance of the evidence standard to proving reasonable danger of harm. The Court noted too that Government had "delineated those portions of its case that involve" the materials at issue. The judge ultimately ordered closure for any time it was reasonably expected that the classified content of the protected exhibits or testimony must be displayed or discussed, must be directly referenced during argument or testimony, or must be referenced by the court on the record. See Enclosure 5.

⁵ As courtroom closure issues were not raised on appeal, the citation offered here is provided so the Court may reference background information for and appellate consideration of the case. It is not intended as a citation for the closure employed in the original trial.

⁶ MRE 506 does not explicitly authorize courtroom closure and MRE 505 does. Therefore, to close pursuant to MRE 506, the Court would have to fully explore the contention that MRE 506 information constituted an overriding interest under RCM 806, whereas, to close the courtroom pursuant to MRE 505, the court just has to be convinced, by a preponderance of the evidence, that the evidence is properly classified and thus deserves MRE 505(j) protection. In the face of that burden, the United States acknowledges that just like in *Anderson*, a Court considering closure may wish to consider witness testimony for MRE 506 information because it is not self-evident or easily understood as warranting protection, yet can rely on classification markings and substantiating documentation such as classification reviews and classification guides for MRE 505 information.

⁷ This request to close the court to hear classified information appears from the closure order to have been made orally before the court. The United States has been unable to find reference to this oral request in the unclassified record of trial in its possession. A written request was found as an appellate exhibit however. See Enclosure 4.

- **Disposition:** Although the case was considered by an appellate court, neither did the accused raise nor did the appellate courts consider public trial issues during their review of the case record. CAAF affirmed.
- **Proposition:** Like the other closure cases, *Anderson* suggests that when the content of classified information is put forward closure is warranted. Further, it highlights *preponderance of the evidence* as the standard to which the Government must prove that the information at issue was properly classified and can reasonably be expected to result in harm if improperly disclosed. Finally, the closure order notes the Government had delineated where it expected the information to be involved in its case. In this case, the United States has done more – delineating not only where the information will be elicited witness by witness, but at what stage of the case, to what level of detail, and to what relevant end. See AE 505.

United States v. Diaz, 69 M.J. 127 (C.A.A.F. 2010) and *United States v. Diaz*, 2009 WL 690614 (N.M.C.C.A. 2009)⁸

- **Misconduct and Outcome:** The accused plead guilty to violating a lawful general regulation, conduct unbecoming an officer, as well as unauthorized removal and wrongful communication of classified information.
- **Closure:** The trial judge closed the courtroom to hear the classified testimony of two witnesses regarding the same classified document.
- **Justification:** In considering the overriding national security interest proffered to warrant courtroom closure, the judge considered: the assertion of classified information privilege by the Deputy Secretary of Defense, a memorandum by the Original Classification Authority (OCA), the declaration of the person (also one of the witnesses) who determined the document at issue was properly classified, as well as the relevant classification guide and associated instructions. The judge articulated findings which: identified the classified document to be discussed, supported the conclusion that the document had been properly classified, stated that serious national security damage could be reasonably expected based on the document's classification designation, explained that closure would occur for each of two witnesses, noted no defense objections to courtroom closure to protect classified information, and inferred that defense cross-examination would likely also elicit classified information. His conclusions mirrored these findings – articulating too that the document had been classified, was relevant to the case, and required courtroom closure for classified discussion. The conclusions also stated that the Judge had conducted the proper balancing analysis and found the interest to be overriding. Lastly, the conclusions explained that alternatives would be used to the extent possible but also that they would not allow for the classified content to be adequately presented and explored. Court closure was “necessary to permit a contextual and complete understanding of the classified testimony”, allow for effective cross-

⁸ As courtroom closure issues were not raised on appeal, these citations are provided so the Court may reference background information for and appellate consideration of the case. They are not intended as citations for the closure employed in the original trial.

examination, and permit clarification if necessary. Moreover, the judge highlighted that the testimony would be bifurcated - presenting classified information during closed sessions and unclassified information during open session. During the open session, the witness could explain unclassified details such as background, biographical information, and an unclassified summary of his testimony. The closed session, he concluded, could include only so much unclassified information as necessary to preserve the coherence of the classified testimony. Finally, in addition to ordering closure for the Government's case-in-chief, the judge preserved the opportunity to do so again should the defense's case necessitate it. *See* Enclosure 1.⁹

- **Disposition:** Though considered twice by appellate authorities (one in a published opinion), neither did the accused raise nor did the appellate courts consider public trial issues during their review of the case record.
- **Proposition:** This closure order helps showcase four things. First, in it, the judge discusses the limitations of affidavits, unclassified summaries, and unclassified testimony as alternatives to classified testimony in closed session. This is similar to the judge's discussion of redactions in *Steele* and *Ledford*. And, it is consistent with the Government's explanation of alternatives in its original *Grunden* filing. *See* AE 480. Second, and relatedly, this closure order anticipates that the closed classified sessions may include such unclassified material as necessary to preserve the coherence of and ensure context for the classified information. This is consistent with the actions in *Lonetree*. It demonstrates that a closed classified session can include unclassified information without ceasing to be narrowly tailored. Third, in a way also consistent with *Lonetree*, this closure order identifies bifurcation as an important tool for courts to demonstrate discretion and their use of the *Grunden* "scalpel." In fact, in *Grunden*, the court writes "bifurcated presentation of a given witness' testimony is the most satisfactory resolution of the competing needs for secrecy by the government, and for a public trial by the accused." *Grunden* at 123. In its original *Grunden* filings, the United States specified closure was only sought for those portions of the testimony which are classified. *See* AE 480 and 506. In so doing, the United States is recognizing and requesting bifurcation as an important "scalpel." Fourth, like *Steele*, this closure order is instructive as it emphasizes open applicability of these findings to whatever witnesses may need to testify about the classified information considered. Consistent with *Lonetree*'s explanation that specific findings are not required witness-by-witness or method-by-method, the order recognizes that witnesses other than those specified in the motion at issue may require protection. The judge notes that a party should notify the court of information "which might necessitate additional closed sessions."

United States v. Ledford, US Navy Southwest Judicial Circuit (2005)

- **Misconduct and Outcome:** The only material in the prosecution's possession regarding this case is the judge's closure order. As no appellate information is available nor is the record of trial in the Government's possession, it cannot provide further background information on this case.

⁹ The *Diaz* Court's protective order, Enclosure 6, and the Prosecution's motion, Enclosure 7, are also included for the Court's reference

- **Closure:** The judge ordered closure for the introduction of classified evidence – occurring only during the portions of a witness’ testimony in which it was reasonably expected that the classified content of the protected exhibit or testimony must be displayed or discussed. The court specified closure for identity-protected witnesses, classified linkages between persons and missions, classified video footage, and classified document contents.
- **Justification:** In this case, two Article 39(a) sessions were held for the parties to make argument and present evidence on courtroom closure. The judge’s findings articulated the general type of information being protected (i.e. “discussions or viewings of tactics/rolls/locations”), how that information would be protected, and what general harm was risked if the information was revealed (i.e. “would reveal foreign government information [and] intelligence sources and methods”). The findings demonstrated their considered nature by specifying that alternatives would be used until the classified content needed to be discussed. Finally, the findings explained that the judge’s review of the evidence with the accompanying classification declarations reveal that the Government had established by a preponderance of the evidence that classification was proper. The judge’s conclusions explained: the rights at stake; the burden on the Government to show the classification and reasonable danger posed by disclosure of the information at issue; that the judge had conducted the required analysis; and that the evidence was relevant, necessary, and otherwise admissible. The actual closure “order” section stated alternatives would be used according to the purpose they serve but that courtroom closure would be used whenever the classified content required exploration. Additionally, this section explained generally the order in which the classified and unclassified sections would occur. Finally, the judge required only that the counsel notify the court prior to opening statements which witnesses they anticipated required court closure and then notify the court prior to eliciting the information that that discussion was coming. *See* Enclosure 8.
- **Disposition:** The United States has found no evidence that this case has been appealed.
- **Proposition:** This closure order is helpful in that it demonstrates how a judge can really focus his or her ruling on the information warranting protection. Doing so is consistent with the information-centric emphasis explained in *Lonetree* and exemplified by *Steele*. Further, in providing information-centered findings, the order also demonstrates the extent to which alternatives such as screens and shields are limited. It shows they are useful if what needs hiding is visual, but not if the information to be protected is oral content warranting exploration. This is consistent with the Government’s discussion of alternatives in its initial *Grunden* filing. *See* AE 480. Also, this closure order highlights that the Government need only convince the Court of proper classification and of reasonably expected harm by a *preponderance of the evidence*. That the judge relied on a review of the evidence and OCA declarations, suggests he did not feel the need to call witnesses to testify during the closure hearing. Finally, this order is useful as it explains the Court only expected information on anticipated witnesses affected before opening statement and an alert when closure was imminent during testimony. Consistent with the

above-described *Steele* case, there is no requirement that the Court nail down exactly and finally which witnesses require closure and know exactly where in the examination that will occur. Such an approach is also consistent with an information-centric and not a witness- or method-centric approach as advocated in *Lonetree*.

United States v. Anzalone, 40 M.J. 658 (N.M.C.M.R. 1994)

- **Misconduct and Outcome:** In this espionage case, the accused was a Marine charged with a variety of offenses arising, primarily, out of his contact with an FBI agent whom appellant believed was a Soviet Union intelligence officer.
- **Closure:** The proceedings were periodically closed to the public. The closure ultimately amounted to 79 pages of the 479 page record, or approximately 16%.
- **Justification:** The Court held the closure requirements had been met. It focused on the probability of the prejudice and the limited nature of the closure. It stated that likelihood of prejudice was established through descriptions of the classified information (in this case, affidavits). As the trial was closed only when the defense or trial counsel anticipated discussing classified matters, the closure was appropriately limited. The United States has been unable to locate any further information showing what the affidavits contained or how the lower court judge actually ordered the closure.
- **Disposition:** The closure findings of the lower court were affirmed.
- **Proposition:** This case shows that like those described above the trial court need not hear testimony about the information before ordering courtroom closure, but rather can rely on affidavits. Moreover, it suggests that by closing only where counsel anticipated classified information to surface, the trial court made an acceptable effort to close no more broadly than necessary.

United States v. Martin, 2012 CCA LEXIS 848 (N.M.C.C.A. 2012) and *United States v. Martin* 2012 CAAF LEXIS 427 (C.A.A.F. 2012)¹⁰

- **Misconduct and Outcome:** Intending to use his lawful access to classified national defense information to reap personal monetary benefit, the accused was apprehended surrendering state secrets to a “Chinese government official” (in fact an undercover FBI agent). The defendant pled guilty to multiple specifications of espionage and gathering defense information in violation of UCMJ Articles 106(a) and 134.
- **Extent of Closure:** According to the prosecuting trial counsel in this case, the Government’s entire sentencing argument occurred in a SCIF based on the highest classified nature of the information.

¹⁰ As courtroom closure issues were not raised on appeal, the citation offered here is provided so the Court may reference background information for and appellate consideration of the case. It is not intended as a citation for the closure employed in the original trial.

- **Justification:** As neither the accused raised his Sixth Amendment right nor did the media or general public attempt to attend, public trial issues did not arise for consideration by the military trial judge.
- **Disposition:** The accused did appeal to the Navy Marine Court of Criminal Appeals (see above citation) on the severity of his sentence. The NMCCA considered the record and was convinced the punishment received was deserved. Accordingly, the appellate court affirmed the lower court's findings. The Court of Appeals for the Armed Forces denied review.
- **Proposition:** While public trial issues in this case were not litigated, it is worth noting that the appellate authority also declined to raise them. According to Federal case law, as a Constitutional question, whether public trial rights have been violated is reviewed *de novo*, and the specific findings of the Court regarding the closure are reviewed for abuse of discretion. See *Hearst* at 174-75; see also *Short* at 44; *United States v. Smith*, 426 F.3d 567, 571 (2nd Cir. 2005); *United States v. Shyrook*, 342 F.3d 948, 974 (9th Cir. 2003); *United States v. Hitt*, 473 F.3d 146, 156 (5th Cir. 2006). And so, it stands to reason, that had the appellate court, in reviewing the record, considered the closed-off nature of the facility to have implicated the public or the accused's constitutional rights, it could have elected to have evaluated those circumstances against the constitutional requirement for a public trial. They did not.

United States v. Lonetree, 31 M.J. 849 (N.M.C.M.R. 1990) *aff'd* *United States v. Lonetree*, 35 M.J. 396 (C.M.A. 1992), and *cert. denied*, 507 U.S. 1017 (1993).

- **Misconduct and Outcome:** The accused was a Marine convicted by general court-martial of identifying United States intelligence personnel to Soviet agents, providing plans and assignments of US embassy personnel, and failing to report contacts with communist citizens.
- **Closure:** The Military Judge excluded the public from the complete testimony of some witnesses and portions of others. The accused alleged this amounted to 25% of the testimony.
- **Justification:** During the original case, the Government presented two affidavits in support of its request for closure. The first, classified "SECRET," explained that witnesses to be called by the government were professional intelligence officers who would provide testimony on classified matters. It also listed the government's rationale for requesting that they testify in closed session. The United States could find no information on how that rationale was articulated. The Government also sought to protect certain specified intelligence sources and methods. The judge in the lower court case conducted his own analysis of these materials. In reviewing that court's closure, the NCMCMR ruled in favor of the Government – finding that the military judge properly analyzed and balanced the competing interests before ordering the closing of the court to the public when specified classified information was to be presented. The NCMCMR wrote:

We do not believe *Grunden* mandated judicial findings for each closed session when the Court of Military Appeals stated that "limited portions" of a court-martial may be partially closed despite defense objection . . . [but rather for] individualized decision-making as to specific information which the Government asserts must be exempted from disclosure at a public trial whenever that information is presented during the course of the trial.

It explained that, because MRE 505 focuses on the information at issue, specificity must occur with respect to the information and not necessarily the method of its disclosure. This stands in contrast to closure for something like an individuals' privacy rights where the interest being protected will vary according to the personal situation of each witness. And so, after classification of a witness' response had already been determined, to make "specific findings each time a series of questions is to be asked of a witness . . . would be to create unnecessary and disruptive bifurcation of the trial and constitute an exercise in redundancy." The resulting confusion, the Court stated, "would make a difficult trial an incomprehensible one and would be the antithesis of a fair and orderly proceeding". In the case of *Lonetree*, the appellate court also found that the procedure the lower court followed was "the fairest and most practical that could be devised." Namely:

The extent of the closures was determined by either Government or defense. (sic) The military judge had already determined which information, because of its classified status, would be presented in closed sessions. The fact that certain unclassified information was disclosed by individuals whose duties and identities could not be publicly matched-up was necessary to protect classified information. Further bifurcation of other witnesses' testimony, other than as occurred, was impracticable and would have created unnecessary chaos. In fact, the apparent inadvertent disclosure of classified information by both parties in public sessions occurred rather frequently despite the efforts of the court to ensure nondisclosure. The procedure utilized allowed both parties a reasonably normal context within which to pursue their respective position.

- **Disposition:** The accused appealed the trial court's closure decision to the NCMCMR claiming, among other things, that the judge erred in failing to find specific overriding national security interests for each closure and in failing to narrowly tailor each closure. This NCMCMR held that each closure did not require findings and that the closures were adequately tailored. The case was then reviewed by the Court of Military Appeals on other grounds. Its review did not disturb the public trial portions of the NCMCMR's ruling. The United States Supreme Court denied certiorari.
- **Proposition:** This case is highly instructive. It emphasizes the need to consider cases on an individual basis. It explains that specific findings aren't necessary for every closure

and goes on to explain that what matters is whether the information warrants protections. It demonstrates the persuasiveness of affidavits. And finally, it highlights bifurcation as an important scalpel tool.

CONCLUSION

The foregoing digest of cases provides a snapshot of how previous judges have handled courtroom closure. They highlight that courts have endeavored to use alternatives and bifurcation to balance the public trial rights against, but have nonetheless closed proceedings to allow witnesses to contextualize, discuss, and clarify classified information at stake. These sessions have included unclassified information to the extent necessary to preserve the coherence of the classified testimony. The United States has found no indication that the parties have ever had to present examination questions in advance. Neither does there appear to be any authority behind having a witness testify during a *Grunden* hearing to test the viability of alternatives. Doing so would, the United States maintains, offend the need to consider information more than method of elicitation or source when deciding whether protection is warranted in the first place. Moreover, it would hardly promote judicial economy because the degree to which alternatives may or may not work for one witness' testimony cannot inform the degree to which they will work for another testifying to separate information and in a different manner. Military appellate authorities trust trial judges to make these decisions – requiring primarily that the courts simply engage in the appropriate analysis. Courts must evaluate the principles and interests at stake, consider possible alternatives, and articulate findings adequately supporting their decision on closure. Yet they need not note specific findings each time the closure actually occurs. It is the United States' position that the evidence and classification reviews coupled with the proffered testimony provides more than enough information for the Court to safely rule to close the courtroom.



JEFFREY H. WHYTE
CPT, JA
Assistant Trial Counsel



ASHDEN FEIN
MAJ, JA
Trial Counsel

8 Enclosures

1. *Diaz* Closure Order
2. *Steele* Redacted Transcript Excerpt
3. *Steele* Unredacted Transcript Excerpt *ex parte* ["SECRET//REL TO USA, MCFI"]

4. *Anderson* Government Motion
5. *Anderson* Closure Order
6. *Diaz* Courtroom Protective Order
7. *Diaz* Government Motion
8. *Ledford* Closure Order

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 29 March 2013.

A handwritten signature in black ink, consisting of a large, stylized loop followed by a series of smaller, connected strokes that trail off to the right.

ASHDEN FEIN
MAJ, JA
Trial Counsel

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Government Targeted Brief
on Courtroom Closures

Enclosure 1

29 March 2013

Encl 1 to
APPELLATE EXHIBIT 511
PAGE REFERENCED:
PAGE OF PAGES

UNCLASSIFIED

DEPARTMENT OF THE NAVY
GENERAL COURT-MARTIAL
NAVY-MARINE CORPS TRIAL JUDICIARY
CENTRAL JUDICIAL CIRCUIT

UNITED STATES

v.

MATTHEW M. DIAZ
LCDR, JAGC, USN

CLOSURE ORDER

1. This matter comes before the Court pursuant to the Government Motion for Appropriate Relief Pursuant to M.R.E. 505 (Appellate Exhibit I) to close certain proceedings in the above captioned case. The defense did not file a responsive pleading, but has filed its own Defense Notice M.R.E. 505 (Appellate Exhibit LXIX).

2. The court considered the Assertion of Classified Information Privilege of Deputy Secretary of Defense, Gordon England dated 15 November 2006 (Appellate Exhibit 65); the memorandum of the Original Classification Authority (OCA), dated 14 August 2006 (Appellate Exhibit 57, Encl. F); and the Declaration of Paul B. Rester, Director of the Joint Intelligence Group, Joint Task Force Guantanamo Bay (JTF-GTMO), dated 21 April 2006 (Appellate Exhibit I, Encl. B). The court also considered the JTF-GTMO Classification Guide of 1 December 2006 (Appellate Exhibit LXIII (sealed)) by which classification of the document at issue is principally governed; and Appellate Exhibits LXI and LXII (sealed), which contain guidance implemented by Appellate Exhibit LXIII. The court enters the following:

Findings of Fact.

1. Appellate Exhibit LXIV (sealed), is a copy of the document at issue in this case (hereinafter "JDIMS list") (also referred to as Enclosure "A" to Appellate Exhibit 57 (not attached to that exhibit)). That list contains the names of GTMO detainees and related data fields.
2. Mr. Paul Rester has 30 years of experience in the intelligence and security field and he is presently the Director, Joint Intelligence Group, JTF-GTMO.
3. Mr. Rester has reviewed the JTF-GTMO Classification Guide and determined that the JDIMS list is currently properly classified SECRET.
4. The OCA concurred with the determination of Mr. Rester.
5. The Deputy Secretary of Defense reviewed the declaration of Mr. Rester and the OCA concurrence, determined that the JDIMS list is properly and currently classified SECRET,

UNCLASSIFIED

APPELLATE EXHIBIT LXIX
PAGE 1 OF 4
APPENDED PAGE _____

and invoked the M.R.E. 505 classified information privilege over disclosure of the list in open court.

6. In addition to having provided a declaration, Mr. Rester will be a witness in this case. Mr. Robert Kates will also testify. The testimony of both men during the government's case-in-chief will include information regarding the classified data fields contained in the JDIMS list and will necessarily include a discussion of information classified at the SECRET level.
7. Disclosure of the SECRET information contained in the JDIMS list and in the witnesses' testimony regarding that information is reasonably expected to cause serious damage to national security. However, not all of their testimony will contain classified information.
8. The government has tendered the following order of presentation: Mr. Rester, followed by several other witnesses providing unclassified testimony, and then testimony by Mr. Kates. This order of presentation is necessary not only to establish the relevance of Mr. Kates' testimony, but also to permit a contextual and complete understanding of the classified testimony of both men. This order of presentation would necessitate two closed sessions, one for each witness.
9. The defense has not objected to the classified testimony being received in a closed session at this court-martial, but the defense has reserved any objection to the testimony of the witnesses on the basis of relevancy or other evidentiary objections.
10. Additionally, the defense has served notice of their need to present the JDIMS list to the members for examination, to inquire into an explanation of the data fields contained therein, and to demonstrate a working model of the JDIMS database. These matters the defense expects to introduce principally through cross-examination of Mr. Rester and Mr. Kates.

Conclusions.

1. The JDIMS list at issue in this case, in its present format, is currently properly classified SECRET.
2. The testimony of Mr. Rester and Mr. Kates regarding the JDIMS list is relevant because it relates to the classified nature of the list, how the JDIMS database works, and the classification status of the JDIMS list at the time it was released. The classified status of the document is an element of Charges I and II and is a factor that members may consider in determining whether the information contained in the list is national security information. An explanation of the nature of the information in the JDIMS list is also relevant for the members to determine whether the list is national security information, whether or not it was classified at the time of its release.
3. The prosecution has sustained their burden of persuasion that closure of this court-martial during the classified testimony of Mr. Rester and Mr. Kates is necessary in the interest of

national security and the proposed closure shall be as narrowly tailored as is possible, as more fully set forth below.

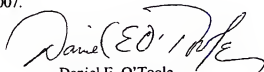
4. This court has carefully balanced the constitutional mandate for the conduct of public trials, and the accused's right to a public trial, against the potential serious damage to the national security of the United States that would result from the public disclosure of SECRET testimony related to the JDIMS list in an open session of this court-martial.
5. The court concludes that the need to protect from disclosure the SECRET information contained in the JDIMS list, and the classified testimony related thereto, outweighs any danger of a miscarriage of justice that could attend the taking of that limited testimony in closed sessions of this court-martial, particularly when the accused has not objected to the closed sessions.
6. The testimony of both witnesses can be bifurcated between classified testimony and unclassified testimony, the latter including biographical and professional background information, the unclassified factual basis for the classified testimony, and an unclassified general summary of the classified testimony concerning the JDIMS list.
7. The bifurcating of testimony between unclassified and classified information properly and narrowly limits the closed session to only the classified portions of testimony and to the limited unclassified supporting information that is necessary to preserve the coherence of testimony during the closed session. However, to present the evidence in the manner most conducive to the court members understanding it, it will be necessary to have one closed session for each witness, with several other witnesses testifying in open session during the period between closed sessions.
8. The court considered alternatives to receiving classified testimony, including use of classified affidavits, unclassified summaries of testimony or unclassified testimony regarding the JDIMS list. A classified affidavit regarding JDMIS would not allow the court members to seek clarification of the technical matters being raised about the database. Even if classified affidavits could be initially used, undue delay in proceedings to seek additional affidavits would be required for any clarification. Use of affidavits would not permit the accused an opportunity to cross-examine the affiants or to present a working demonstration of the JDIMS database. Unclassified testimony or unclassified summaries would not adequately provide the court with the requisite level of detail needed to accurately assess the nature and status of the JDIMS list, which is at issue in all charges. As a result, the alternatives to classified testimony are inadequate even when compared to receipt of testimony in closed proceedings.
9. In bifurcating classified from unclassified testimony, the court seeks to provide the maximum public access to these proceedings consistent with national security. Additional protective measures, short of closure, will permit the introduction and use of classified documentary evidence relating to the testimony of the witnesses during open sessions of the court, and will further limit the need for, and the duration of, closed sessions.

UNCLASSIFIED

Ruling.

1. It is hereby ORDERED that the classified testimony of Mr. Rester and Mr. Kates regarding the JDMIS list, and only so much of their unclassified testimony as is necessary to preserve the coherence of their classified testimony, shall be taken in separate closed sessions, one for the examination of each witness. These closed sessions will be held during the government's case-in-chief and will include direct and cross-examination.
2. The defense shall notify the court pursuant to M.R.E. 505 of any intention to introduce any classified information during the defense case-in-chief, which might necessitate additional closed sessions.
3. Open and closed sessions of this court will be conducted in accordance with the further requirements of the Court Room Protective Order of this court, issued separately this date.

Entered this 11th day of May 2007.



Daniel E. O'Toole
Captain, JAG Corps, U.S. Navy
Circuit Military Judge

UNCLASSIFIED

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Government Targeted Brief on Courtroom Closures

Enclosure 2

29 March 2013

Encl 2 to
APPELLATE EXHIBIT 511
PAGE REFERENCED: _____
PAGE _____ OF _____ PAGES

1 MJ: Do you understand that even though you believe you are
2 guilty, you have the legal and moral right to plead not guilty and to
3 place upon the government the burden of proving your guilt beyond a
4 reasonable doubt?

5 ACC: Yes, sir, I understand that.

6 MJ: Lieutenant Colonel Steele, take a moment now and consult
7 again with your defense counsel and then tell me whether you still
8 want to plead guilty.

9 [Accused complied.]

10 ACC: Yes, Your Honor, I still want to plead guilty to the
11 three charges I pled guilty to.

12 MJ: Lieutenant Colonel Steele, I find that your plea of
13 guilty is made voluntarily and with full knowledge of its meaning and
14 effect. I further find that you have knowingly, intelligently, and
15 consciously waived your rights against self-incrimination, to a trial
16 of the facts by a court-martial and to be confronted by the witnesses
17 against you. Accordingly, your plea of guilty is provident and is
18 accepted. However, I advise you that you may request to withdraw
19 your guilty plea at any time before the sentence is announced, and if
20 you have a good reason for your request, I will grant it.

1 Trial counsel, is the government going forward on any of the
2 charges or specifications to which the accused pled not guilty or the
3 excepted language?

4 ATC2: Not the excepted language, Your Honor, however, all other
5 charges that were not dismissed prior to referral, we are going
6 forward.

7 MJ: So all the remaining charges and specifications but not
8 the excepted language? Okay, thank you.

9 ATC2: Yes, sir.

10 MJ: In that case, I will not enter findings at this time.

11 The trial is set for 0900 hours on 15 October. There will be an
12 Article 39(a) session to litigate motions and issues concerning
13 Military Rule of Evidence 505 and Military Rule of Evidence 506 on 12
14 October at 0900 hours.

15 Counsel, are there any issues to address before the court
16 recesses?

17 ATC2: No, sir.

18 DC: No, sir.

19 MJ: The court is in recess.

20 [The Article 39(a) session recessed at 1629, 7 October 2007.]

21 [END OF PAGE.]

1 [An Article 39(a) session was called to order at 0908, 12 October
2 2007.]

3 MJ: This Article 39(a) session is called to order. All
4 parties present on 7 October 2007 are again present and no additional
5 parties are present today.

6 Now counsel, I just want to check, I had thought that at prior
7 Article 39(a)s before October 7th there might have been security
8 officers for each side, is that correct? Trial counsel, do you have
9 a security officer appointed on your side?

10 ATC2: Yes, sir, and just for clarification for the record,
11 Captain Inurell Chester for the government is the court security
12 officer and Major Dennis Daniels, the defense----

13 MJ: And that's exactly why I was asking.

14 ATC2: It's the only change that's occurred since 7 October,
15 sir, in terms of accounting for the parties.

16 MJ: And they're behind the bar, that's why I'm asking to see
17 if they are here. So, all parties present on 7 October are again
18 present and the two additions are Captain Chester and Major Daniels
19 are both present in the courtroom.

20 Prior to coming into the courtroom today, I conducted an R.C.M.
21 802 conference, present were the seven counsel and myself, and we
22 discussed marking of the documents, which was kind of painful, how

1 those were going to be marked, but I think we worked through a system
2 where we can get them marked appropriately, and we'll find that out
3 as we go along today.

4 Do counsel for either side have any objections, corrections or
5 additions to my characterization of the R.C.M. 802 conference?

6 ATCl: No, Your Honor.

7 DC: No, sir.

8 MJ: And also during the R.C.M. 802 conference, counsel let me
9 know that the witnesses for an Article 13 motion weren't going to be
10 ready until the afternoon. So what we're going to do is we're going
11 to handle the *Grunden* hearing first and then we'll deal with the two
12 motions that are still pending, those are a motion to dismiss, we'll
13 do that first as far as the motions, and then the Article 13 motion
14 we'll do second.

15 Also, the defense hasn't had an opportunity to compare a
16 redacted version of some documents that they were intending to offer
17 with the unredacted version to see what impact that has on what they
18 were wanting to offer. They're going to need that when we litigate
19 that part of the *Grunden* hearing. So, I anticipate that after we get
20 started in a little while, I'm going to have to give a decent length
21 recess for the defense counsel to accomplish that before we move on.
22 But what I want to do is we're going to get started with the *Grunden*

1 hearing so I'm going to close the court based on the motion by the
2 parties for this *Grunden* hearing is the reason for the court to be
3 closed. So what we're going to do is we're going to change and go
4 into a closed session and then the only ones that will be present
5 will be the seven counsel, the three court security officers, the
6 court reporter and myself. And just for the record, there's only one
7 other person in the courtroom right now that that affects and then
8 she's going to have to leave the courtroom. So what we're going to
9 do is take a brief recess to accomplish that.

10 The court is in recess.

11 [Court recessed at 0912, 12 October 2007.]

12 [The next session is a closed session which contains pages 249
13 through 312 and is contained in the original record of trial, only.
14 The next numbered page of the unclassified portion of this record of
15 trial is page 313.]

16 [END OF PAGE.]

[REDACTED] [REDACTED]

1 (U) [An Article 39(a) session was called to order at 0912, 12 October
2 2007.]

3 (U) MJ: Court is called to order. All parties present before
4 the court recessed are again present. And just for the record, the
5 court is closed now. The only parties present are the parties I
6 mentioned a little while ago.

7 (U) And during the recess, the trial counsel stated that the
8 bailiff had a proper security clearance, if I wanted her in the
9 courtroom. I just found that she wasn't necessary so she's not in
10 the courtroom.

11 (U) Okay, counsel, so what we're going to do is to conduct a
12 hearing under Military Rule of Evidence 505. There's a couple
13 reasons why a hearing is conducted under Military Rule of Evidence
14 505. Now, I hadn't mentioned when we were conducting the R.C.M. 802
15 conference, I did also ask the trial counsel if they were opposing
16 the defense's offer, the evidence that the defense intended to offer
17 as far as relevance or for any other reason, or if they were just
18 wanting the court to be closed when the defense offered that
19 evidence. And the trial counsel stated that they weren't opposing
20 that the defense could offer that evidence but they just wanted the
21 court to be closed during those portions of the court-martial. Well,

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

1 I mentioned to them, I said, "Well, perhaps with the exception of the
2 evidence that's been redacted, if they could use the redacted version
3 versus an unredacted version, and that's a way in which the court
4 would not have to close as often and ensure a public trial for a
5 greater portion of the trial, which would be in the interest of
6 justice. So, I already mentioned that we're going to give the
7 defense time to review the redacted version and see if that
8 accomplishes what they want, or at least in most part.

9 (U) But anyhow, so what we're going to go do is we're just going
10 to go in to see if there is sufficient reason to close the court
11 during portions of the court-martial. And the way I'm going to
12 handle it, and we've started when I talked with counsel to talk about
13 it, is round one, round two and round three, is the classified
14 information that was processed went up in about three different
15 rounds. The first round has already been marked as Appellate Exhibit
16 XXI, and it contains 20 different documents, 11 that went up to one
17 original classification authority and nine that went up to a
18 different original classification authority. And that was processed
19 relatively early in the court-martial process. And that's round one.
20 (U) Round two consisted of exhibits that we're going to talk
21 about at a later time, but it was copies of documents that the

[REDACTED] [REDACTED]

[REDACTED]

1 defense wanted to use and also some documents that the government
2 wanted to use, and that was contained in three different binders that
3 we will address later. And then three is evidence that went up
4 recently to the Commander of the Multi-National Force, Iraq; I think
5 it went up on 6 October, and that's a smaller round, but that's round
6 three. And so, what we're going to do right now is we're just going
7 to handle round one and then we're going to have to take a recess
8 before we cover round two.

9 (U) What I'll do is I have reviewed all of the documents that
10 are contained within Appellate Exhibit XXI. And counsel, do you have
11 any evidence to present on this issue, trial counsel?

12 (U) ATC1: No, Your Honor.

13 (U) MJ: Defense counsel?

14 (U) DC: No, sir.

15 (U) MJ: I'll allow you to argue then. Trial counsel, go
16 ahead.

17 (U) ATC1: Yes, Your Honor.

18 (U) The standard under M.R.E. 505(3), demonstration of national
19 security nature, requires that the affidavit demonstrates the
20 disclosure of the information reasonably could be expected to cause
21 damage to the national security and the degree caused required to

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

1 warrant classification under the applicable executive order or statute
2 or regulation. In both the 11 and 9 documents contained in Appellate
3 Exhibit XXI, the affidavits completed by Gunnery Sergeant and Captain
4 Gawlick demonstrate that. And again, this was ratified in the OCA
5 memos that are also contained in that exhibit, Appellate Exhibit XXI.
6 So Your Honor, we ask that we close the courtroom for that portion of
7 the trial related to those documents. The government intends to
8 offer two witnesses, Gunnery Sergeant Whalen and Captain Gawlick, who
9 are going to discuss those documents. And while they're discussing
10 those documents--not here today, sir, but at trial. And while
11 they're discussing those documents, we ask that you close the
12 courtroom to the public, Your Honor. Thank you.

13 (U) MJ: Defense counsel, you may argue.

14 (U) DC: Yes, sir. Sir, with regards to these documents and
15 the showing that the government has made in terms of closing the
16 courtroom for testimony with regards to these documents or the
17 presentation of these documents, defense does not object to the
18 closing of the courtroom regarding these documents. However, we do
19 reserve the right to object to foundational objections or other
20 objections of that nature with regards to putting these things into
21 evidence or the testimony that would be elicited.

[REDACTED]

[REDACTED]

1 (U) MJ: Sure, absolutely. I mean, that's a good point.
2 Obviously, the court's not going to admit any of these documents.
3 We're just determining whether or not we're going to receive this
4 evidence in a closed session, that's all.

5 (U) DC: Yes, sir. So, the defense has no objections to
6 receiving the information of this nature related to these documents
7 in a closed session.

8 (U) MJ: Okay. [Pause.]

9 (U) Okay, I'm going to address the documents contained in
10 Appellate Exhibit XXI. First of all, there are 11 documents that
11 fell within the purview of the Commander of Multi-National Force,
12 Iraq. The first document is OPLAN 0601, is a defense plan for Camp
13 Cropper, and it's dated 15 March 2006. It is marked "secret". It's
14 a full OPLAN with the situation, mission, execution, service support
15 and command and signal with annexes that include photographs and
16 diagrams of the camp. Most internal portions are marked "secret" and
17 some are marked "unclassified".

18 ~~(U) Second is a chemical response assessment for Fort Suse, is~~
19 ~~that it?~~

20 (U) ATC2: Yes, sir.

[REDACTED]

[REDACTED]

1 (U) MJ: Suse is how they pronounce it? Okay...dated 9 May
2 2006. It's marked "secret". This five-page document depicts a
3 theater internment facility's ability to respond to a chemical
4 attack. It includes the status of detection assets and
5 recommendations for future CBRN defense for that facility.

6 (U) Third, there is an info brief for the Commander of 4th
7 Infantry Division concerning Camp Cropper; it's dated 6 April 2006.
8 It's marked "secret". These 22 PowerPoint slides show the unit's
9 mission, commander's intent, organization, equipment and facilities
10 and has two detailed diagrams.

11 (U) Fourth is the Charlie 1/142d FA guard force chart and two
12 photos. It's undated; it's marked "secret". This three-page
13 document contains a chart with a number of guards and two aerial
14 photos with captions.

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 [REDACTED]

[REDACTED]

[REDACTED]

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]

4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]

8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]

14 (U) Eighth, a troop to task info brief, it's undated; it's
15 marked "secret". This document contains slides with charts and
16 diagrams showing the staffing, shifts, and layout for an internment
17 facility.

18 (U) Ninth, an update briefing to the Commander of the 43d MP
19 Brigade on the movement of HVC number 1. It is undated; it's marked
20 "secret". These 40 PowerPoint slides show the mission and methods of

[REDACTED]

[REDACTED]

1 movement with the routes, alternate routes, maps and force
2 protection. It also contains slides on visitor issues.

3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]

8 (U) Eleventh, slides with pictures and identities of detainees
9 with classification of "other," dated 27 June 2006. It's marked
10 "secret". It has pictures, identities, ID numbers and in some cases,
11 disposition from adjudication for other detainees separated by
12 category. I find that these eleven documents have been properly
13 classified as secret by the proper original classification authority,
14 which is the Commander of the Multi-National Force, Iraq, which is
15 currently General Petraeus. It also has been done in accordance with
16 Executive Order 12958, as amended most recently on 25 March 2003,
17 specifically sections 1.4 Alpha, 1.4 Charlie and 1.4 Golf.

18 (U) Next, I want to go into the documents that fell within the
19 purview of United States Army Central. First, there is an executive
20 brief from Major General Dunlavey, dated 31 March 2002, marked
21 "secret". These PowerPoint slides focus on detainee operations in

[REDACTED]

[REDACTED]

1 Afghanistan with the concept of the operations, photographs,
2 diagrams, operational issues, and lessons learned.

3 (U) Second, "Detainee Movement Plan," undated, marked "secret".
4 This one-page document contains a map and flight schedules.

5 (U) Third, more of a detainee movement plan, undated, marked
6 "secret". This one-page document contains a map and times.

7 (U) Fourth, an email dated 8 February 2002, marked "secret".
8 This email discusses release of a named detainee.

9 (U) Fifth, Al-Qaeda and Taliban Leadership, undated, marked
10 "secret". This two-page document shows leadership structure of Al-
11 Qaeda and Taliban with pictures, identities and most current status.

12 (U) Sixth, Southwest Asia Air Defense Artillery Update, dated 4
13 April 2002, marked "secret". These PowerPoint slides contain
14 information on the threat and friendly capabilities, including
15 problems with--correction, including problems with recommendations
16 and missile inventory. Internally, most portions are marked "secret"
17 with some marked as "unclassified".

18 (U) Seventh, email dated 21 May 2002, marked "secret". This
19 email contains the number of detainees as reported by the National
20 Detainee Records Center in the Pentagon.

[REDACTED]

[REDACTED]

1 (U) Eighth, detainee report, dated 19 May 2002, marked "secret".
2 This document lists ten detainees by ISN with location, full name,
3 nationality, date of birth, gender, physical condition and
4 information about their capture.

5 (U) And ninth, slides on Coalition, dated 7 February 2007,
6 marked "secret". These PowerPoint slides with comments show and
7 discuss the support that Coalition countries are providing. I find
8 that these documents have been properly classified as "secret" by the
9 proper original classification authority, which is the Commander of
10 the United States Army Central, which is currently Lieutenant General
11 Whitcomb. And I find that this has been done in accordance with
12 Executive Order 12958, as amended most recently on 25 March 2003,
13 specifically sections 1.4 Alpha, 1.4 Bravo, 1.4 Charlie, 1.4 Delta,
14 and 1.4 Golf.

15 (U) From all the evidence, I am satisfied that there is a
16 reasonable danger that presentation of these 20 documents before the
17 public will expose military matters that, in the interest of national
18 security, should not be divulged. Specifically, disclosure in open
19 court would increase the vulnerability of Camps Cropper and Suse. It
20 would decrease the effectiveness of current military operations in
21 Iraq. It would increase the vulnerability of Coalition Forces

[REDACTED]

[REDACTED]

1 against chemical attack. It will jeopardize the relationship that
2 the United States has with friendly and Coalition Forces. It will
3 endanger the lives and safety of Coalition Forces and it will
4 decrease the effectiveness of intelligence collection during the
5 current operations.

6 (U) Counsel, the next part is just to discuss how that
7 information is going to be disclosed in court. And what I'm willing
8 to do is we can talk about the information first and all the
9 different rounds, and then we can go by witnesses if witnesses are
10 going to discuss information in multiple rounds. Or, if it's easy
11 and this evidence is just going to come out through a specific
12 witness or just in documentary form, then we can discuss that now.
13 Trial counsel?

14 (U) ATCl: Sir, for those documents that you've just discussed,
15 for the MNF-I documents, the government intends to call Captain
16 Gawlick to offer testimony as to how those documents relate to the
17 national defense and how they could be used to the injury of the
18 United States or to the advantage of a foreign nation as an element
19 of the 18 USC 793 Echo charge. So, probably what we expect at this
20 point is that Captain Gawlick will testify as to the specifics of
21 those documents as it relates to those two elements of that offense.

[REDACTED]

[REDACTED]

1 The same thing for Gunnery Sergeant Whalen, Your Honor, we intend to
2 call him and to offer similar testimony, how they relate to the
3 national defense and how they could be used to the injury of the
4 United States.

5 (U) MJ: Now for those two witnesses, is that the only thing
6 that they're going to talk about?

7 (U) ATCl: Yes, Your Honor. And Your Honor, if I may just add
8 on one other thing.

9 (U) MJ: Sure.

10 (U) ATCl: We'll argue that in closing, as well, so it will come
11 out in the closing argument, as well.

12 (U) MJ: Okay, so in closing, you're going to talk about the
13 actual contents of each of these documents, okay.

14 (U) Trial counsel, any other witnesses going to talk about these
15 documents, foundational witnesses?

16 (U) ATCl: Yes, Your Honor. And there's really one of two ways
17 we could do that for the foundational witnesses. We could put a

18 "secret" cover on the documents to show them or to have them look at
19 that on the stand without revealing it to anybody who happens to be
20 in the court and then testify that, "Yes, I found this particular

[REDACTED]

[REDACTED]

1 document on this particular CD," or "I found this particular document
2 in----"

3 (U) MJ: So they're going to authenticate it as a document
4 that they found somewhere, but they're not going to talk about the
5 content.

6 (U) ATC1: The substance of what's in the document, roger, sir.

7 (U) MJ: So you're not asking to close any portion of those
8 foundational witnesses' testimony, are you?

9 (U) ATC2: We don't think it's necessary, Your Honor, but if you
10 don't want us to put a "secret" cover on that and give it to the
11 witness like that, we can----

12 (U) MJ: There's no problem having a "secret" cover on there.
13 If it's supposed to have a "secret" cover, then it can have a
14 "secret" cover. No, I understand, it appears to be no need for you
15 to go into the contents of it so there's no need to close any portion
16 of that foundational witness' testimony. But these other two
17 witnesses that that's all they're going to talk about and these
18 documents are all "secret," defense counsel, do you want to be heard
19 on that as far as whether or not these documents are going to be
20 addressed by any other witnesses?

[REDACTED]

[REDACTED]

1 (U) DC: Sir, as far as we can see right now, none of the
2 defense witnesses are going to address the contents of those
3 documents.

4 (U) MJ: All right, well based on that, for the two witnesses
5 that are going to talk about the impact of these, their only
6 testimony is going to be about these documents. Apparently, one will
7 talk about 11 documents and the other will talk about 9 documents.
8 That's going to be the only testimony that those witnesses provide.
9 I don't see any way in which any of their substantive testimony can
10 be conducted in open court based on the nature. It has been clear, I
11 fully read all those documents and it just can't be discussed in open
12 court without risking national security. However, what I do want to
13 do because I'm balancing the right to a public trial with the
14 interest of national security, is even if a witness is going to
15 testify only about classified information, that's all the substantive
16 information, to the public, it is in their interest for a public
17 trial that they at least know who is in here testifying. So although
18 it may be a logistical pain for certain people, but what I do want to
19 do is when that witness is called, the court will be open. So the
20 witness will come in. The witness will take the oath. The witness
21 will state the name, unit, etcetera, do any foundational requirements

[REDACTED]

[REDACTED]

1 as far as who this person is. And then once the trial counsel is
2 getting into the documents, at that point, you can close...you can
3 ask that the court be closed at that point.

4 (U) Trial counsel, are you tracking where I'm going?

5 (U) ATCl: Yes, Your Honor.

6 (U) MJ: I see that as it's different than if the members of
7 the public can't even see who's being brought in here, it looks like
8 a secret star chamber in here and that's not what we want. We want
9 the public to be able to view everything that they can view, and I
10 think that accomplishes that for those witnesses. As far as the
11 other witness, I see no need to close any portion of the foundational
12 witnesses' testimony based on what we know right now. So, none of
13 that testimony will be conducted in closed court.

14 (U) ATCl: Sir, if I may?

15 (U) MJ: Sure.

16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]

[REDACTED]

[REDACTED]

1 (U) MJ: Are they going to talk about other matters, too, or
2 just these documents?

3 (U) ATC1: Lieutenant Evans, just the document, General Gardner
4 may get into other material, as well.

5 (U) MJ: Let me ask you about Lieutenant Evans' testimony.
6 When he testifies, everyone realizes that the finder of fact has read
7 the documents. Is he going to discuss the contents of the documents
8 or is he going to talk about the impact? And if he's talking about
9 the impact, will it be getting into classified information or will he
10 necessarily have to disclose? I mean, there's two possibilities; I
11 don't know what his testimony is going to be, but I would envision
12 that he could talk about impact without disclosing any classified
13 information. But I also could see a situation where he couldn't.
14 Which do you think it is?

15
16
17
18
19
20
21

[REDACTED]

[REDACTED]

[REDACTED]

1 (U) MJ: So he actually will be getting into classified
2 information.

3 (U) ATCl: Yes, Your Honor.

4 (U) MJ: All right. And is that what's going to be his...his
5 testimony is going to be about site assessment and vulnerabilities?

6 (U) ATCl: Yes, Your Honor.

7 (U) MJ: Okay, I'm inclined to close all that. I mean,
8 knowing exactly what's in the documents and the risk involved,
9 defense counsel, I'm intending to close that portion of his
10 testimony. Do you want to be heard on that?

11 (U) DC: No, sir, we don't have an objection to those portions
12 of Lieutenant Evans' testimony being closed. We would have objection
13 if the complete testimony of General Gardner were closed because we
14 believe that he's going to be testifying about various different
15 matters.

16 (U) MJ: Absolutely, no, I haven't touched that yet because I
17 don't envision closing all his testimony and I think that would be
18 very unlikely.

19 (U) I find that based on the proffer by the trial counsel, all
20 the substantive evidence by Lieutenant Evans about impact of
21 disclosure on site assessment and vulnerabilities must be held in

[REDACTED]

[REDACTED]

1 closed court because it poses a serious risk to national security
2 otherwise. For him, for Lieutenant Evans, obviously we handle it the
3 same way as with the other witnesses I talked about whose testimony
4 was all about classified testimony. He'll still come in, do the
5 initial questions in open court and then only when you're ready to
6 get into the substance of his testimony will we close the court.

7 (U) ATC1: Sir, if I may just jump in there. Lieutenant Evans,
8 his duty position and his existence within the Army may itself be
9 classified. We're trying to run that to ground.

10 (U) MJ: Okay.

11 (U) ATC1: He would be the one witness where that would probably
12 be an exception to the--I understand what you're saying, Your Honor,
13 where the witness comes in----

14 (U) MJ: I understand. I understand duty position. So you're
15 saying even his existence within the Navy?

16 (U) ATC1: Well, the fact that he....

17 (U) MJ: You're saying even his existence that he's in the
18 Navy?

19 (U) ATC1: We're going to have to verify that, Your Honor.

20 (U) MJ: Yes, okay, we can address that later.

21 (U) Do you want to be heard on that, defense counsel?

[REDACTED]

[REDACTED]

1 (U) DC: Yes, sir, his name and position were on--or not duty
2 position, but at least his name was on all the witness lists that
3 were unclassified, so I don't think his identity, itself, is a
4 classified matter. Maybe the nature of his work and what he does, so
5 I think he can at least come in and be identified as a witness and we
6 can just close it as to those duties that would be considered of a
7 classified nature.

8 (U) MJ: Unless you come back with further argument on
9 why...and I understand that there might be an argument why actually
10 his name might be removed from certain lists for a tour of assignment
11 and perhaps there's an argument there but I don't have it in front of
12 me. And I agree with defense counsel, is in that case, perhaps his
13 current assignment, duties, that may be classified. So, where
14 oftentimes you might ask a person their name and then next ask the
15 unit of assignment and then go into their background, but this
16 witness, what you could do, is ask his name. Unless I get a
17 different ruling based on further argument from you, get his name,
18 perhaps how long he's been in the Navy and maybe some of this
19 background. Don't ask his current duty assignment until you get that
20 foundational part done. And then ask for the court to be closed, and

[REDACTED]

[REDACTED]

1 then you can get out his current assignment after the court's closed
2 and then go on from there.

3 (U) Do you understand, trial counsel?

4 (U) ATCl: Yes, Your Honor.

5 (U) MJ: That's my ruling as far as right now. I'm open to
6 reconsider if you come back with an argument that just his name and
7 the fact that he's in the Navy right now is a classified matter,
8 you're going to have to convince me of that beforehand, otherwise my
9 ruling stands as I just stated, okay?

10 (U) Now, as far as Lieutenant General Gardner, trial counsel,
11 what portions...correction, what subject matters is he going to
12 cover? Is he going to cover various sentencing information? Well,
13 first of all, I don't think you asked for Lieutenant General
14 Gardner's total testimony to be closed, is that right?

15 (U) ATCl: No, Your Honor, it would be limited in scope.

16 (U) MJ: All right, now, for the part where he's talking about
17 any of these documents, is he going to have to get into the contents
18 of the documents like Lieutenant Evans will have to?

19 [REDACTED]
20 [REDACTED]
21 [REDACTED]

[REDACTED]

1

2

3 (U) MJ: All right, I see. So he's not just talking about in
4 any hypothetical situation, "When you disclose this type of
5 information, this is the risk," he's going to actually talk about in
6 this specific case, this is the impact that it had? So, he's going
7 to talk about the contents of the documents, themselves?

8 (U) ATCl: Yes, Your Honor.

9 (U) MJ: So, defense counsel, just to expedite matters, I'm
10 inclined to close the portions when he's talking about these 20
11 documents specifically, what was in them and then the specific impact
12 from those. Do you want to be heard on that?

13 (U) ADC: No, sir, I'll likely handle General Gardner's
14 testimony. I agree with your earlier comment about if he's talking
15 impact. I think much of his testimony to be, "This sort of impact on
16 the vulnerabilities was damaging." Maybe there's one or two facts in
17 those documents, but I think it would be fairly limited. You know,
18 "This one slide," you know, "This one particular..." but even that, I
19 think he can say, "One of the slides in there talks about
20 vulnerabilities." So I think as much as possible, we can have that
21 in public forum, limited to the very few facts that he might point to

[REDACTED]

1 in the documents. I mean, I could see where the government might
2 point out one or two things, but the overall impact, I don't believe
3 that would be classified.

4 (U) MJ: Okay, so....

5 (U) ADC: Only when he ties it to a specific fact.

6 (U) MJ: Right, and I think what they're going to do is,
7 that's what I was talking about earlier, it sounds like they're going
8 to be tying it to specific facts. But what you're saying is, when
9 he's all done, and he might be covering more than the 20 documents, I
10 don't know if he's talking about anything else. But when he's all
11 done, he's ready to give an opinion, overall opinion, on what the
12 impact of those documents, disclosure of those documents were, then
13 that could be done in open court. I'm open to that. Like I said, I
14 am wanting to chisel away at the closed portion of this trial as much
15 as possible. So if I can chisel out a single question and answer,
16 then I'm going to do that. And it sounds like the defense counsel is
17 correct in that the overall impact, if you're going to ask a question
18 about what the overall impact was either of these 20 documents, or if
19 you're not doing it just for the 20 but if he's talking about other
20 things and he's going to say the 20 documents plus "X," what's the

[REDACTED]

[REDACTED]

1 overall impact, and you're going to summarize his testimony that way
2 at the end, then that would be able to be accomplished in open court.

3 (U) Trial counsel, do you intend to do that? Do you intend to
4 give an overall impact based on----

5 (U) ATCl: Yes, Your Honor, it probably will be two portions.
6 It would probably be an--I'm sorry, I shouldn't say "would," it will
7 be an overall impact testimony but he will also testify about
8 specific vulnerabilities.

9 (U) MJ: Sure.

10 (U) ATCl: And I understand your ruling, Your Honor, that for
11 the overall arching as it doesn't relate to the details, that that
12 would be in open court.

13 (U) MJ: Right.

14 (U) ATCl: As it relates to the specifics, details within those
15 documents, it would be closed.

16 (U) MJ: Exactly. Okay, that's the ruling of the court. When
17 it's talking about impact from disclosure of these specific documents
18 and he's talking about what's in the documents, that will be
19 conducted in closed court. I find that it's required for the
20 interest of national security. However, when he does give an overall

[REDACTED]

[REDACTED]

1 opinion, what type of impact this caused, then that is able to be
2 elicited in open court and that's how it will be elicited.

3 (U) Okay, I think we've discussed these 20 documents
4 sufficiently so I think counsel for both sides understand what can be
5 discussed in open court, what can be discussed in closed court. Do
6 counsel for either side have any questions on the court's ruling just
7 for this round?

8 (U) ATC1: No questions, Your Honor.

9 (U) DC: No, sir.

10 (U) MJ: All right, now we're ready to move into round two.
11 And to do that, as I mentioned earlier, that defense counsel, you are
12 going to have to compare the redacted and unredacted volumes of the
13 evidence that you gave notice that you intended to offer. And I
14 think you understand the goal there is, if you're able to use
15 unredacted versions of emails or memos or letters, then what happens,
16 if that gets across the point you're trying to get across, then we're
17 able to accomplish that in open court and that's the goal of the
18 court is to do that. As long as we still have a fair trial, that's
19 what I want to do as much as possible is to conduct this in open
20 court.

[REDACTED]

[REDACTED]

1 (U) So as you're going through, do that. However, if you find
2 portions that have been redacted that's really what you were wanting
3 to get at with that document, just make a list and we can focus in on
4 those specific things and perhaps we can, for certain reasons, go
5 into closed court for some of those and we might have some unredacted
6 documents that were within that bigger binder. I just want to focus
7 you in on what I want you to look at during the recess so that when
8 we come back in we can talk in detail about that.

9 (U) I'm going to take a recess. Defense counsel, do you think
10 30 minutes is sufficient?

11 (U) DC: [No verbal response.]

12 (U) MJ: We're going to plan on that now. If you need more
13 time, then just let me know before the 30 minutes is up, does that
14 work?

15 (U) DC: Yes, sir.

16 (U) MJ: The court is in recess.

17 (U) [The session recessed at 0954, 12 October 2007.]

18 (U) [Court reconvened at 1305, 12 October 2007.]

19 (U) MJ: Court is called to order. All parties present before
20 the court recessed are again present. The court is still in a closed
21 session discussing Military Rule of Evidence 505. And as I stated,

[REDACTED]

[REDACTED]

1 all the parties that were present previously are again present; no
2 one else is present at this time.

3 (U) During the recess, I conducted an R.C.M. 802 conference.
4 Present were all seven counsel, all three security officers and
5 myself. We discussed the defense counsels' comparison of the
6 redacted information they had submitted under Military Rule of
7 Evidence 505(h) with the unredacted version. And those had been
8 marked as Appellate Exhibits XXX and XXXI; XXX is unredacted, XXXI is
9 redacted. And also what we're going to be discussing now is
10 Appellate Exhibit XXIX as well as Appellate Exhibits XXXIII and XXXIV
11 because these all relate to information that was processed together,
12 some of them to different original classification authorities. So
13 during the R.C.M. 802 conference, defense counsel articulated what
14 exactly they were going to go into during the trial and that assisted
15 in focusing the parties where we need to go during this Article 39(a)
16 session, and we'll go into that in more detail.

17 (U) And then also, we discussed a couple of other issues. One
18 was privilege under Military Rule of Evidence 506. And the
19 government had provided the court with a memorandum from the Deputy
20 Secretary of Defense, dated 16 February 2006; that's been marked as
21 Appellate Exhibit XXXV. And what we'll do is we'll discuss that at a

[REDACTED]

[REDACTED]

1 later time. Specifically, it's talking about, apparently it's an
2 exercise of privilege in all cases involving specific information,
3 specifically ICRC communications. So the way it's addressed and what
4 it addresses within the memorandum indicates it may be broader than
5 just the one case that's mentioned on the document.

6 (U) Also, we discussed witness issues, specifically there are
7 three witnesses that are currently detainees at Camp Cropper. And,
8 according to the defense counsel, those witnesses, they're going to
9 be produced, but if they're produced, they're not going to say
10 anything. And so we discussed that, and the counsel were talking
11 about having them declared as unavailable. But on further thought,
12 what we're going to need to do, for the court to find them
13 unavailable, the court's going to need some evidence before it to
14 find them unavailable. And if the parties enter into a stipulation
15 about the facts that the court could rely on, but the court is not
16 going to be able to rely on assertions by counsel to make a
17 determination that witnesses are not available. So, the counsel can
18 talk during breaks today and determine if they wanted to enter into a
19 stipulation or if they bring in other evidence to support that if the
20 defense is still wanting to call those witnesses. Or, if there's
21 alternative means that the defense is going to use, they can do that,

[REDACTED]

[REDACTED]

1 also. But the court, to make a determination of nonavailability, the
2 court does have to have evidence in front of it to make that fact
3 specific ruling.

4 (U) Okay counsel, what we're going to do now is we're going
5 to...well, first of all, does anyone have any objections, corrections
6 or additions to my characterization of the R.C.M. 802 conference?
7 Trial counsel?

8 (U) ATC1: No, sir.

9 (U) MJ: Defense counsel?

10 (U) DC: No, sir.

11 (U) MJ: Okay, and we'll go in more detail as I said
12 about...the bulk of the time that we were in there we were going down
13 pretty studiously specific information in Appellate Exhibits XXX and
14 XXXI. But I just want to mention, we had already covered Appellate
15 Exhibit XXI and I just want to say for the record that I did find
16 that the need for excluding the public from portions of the trial
17 that I delineated is of sufficient magnitude so as to outweigh the
18 danger of any miscarriage of justice which may result from judicial
19 proceedings being carried out in even partial secrecy.

20 (U) Also, the 20 documents that were discussed within Appellate
21 Exhibit XXI along with all other classified exhibits that the court

[REDACTED]

[REDACTED]

1 already has will be placed in a separate volume or volumes of the
2 record of trial that will be appropriately marked and handled as
3 classified in accordance with DoD and Army regulations.

4 (U) Also, one thing that I want to ask trial counsel to focus a
5 little bit more on a couple of the witnesses. As far as Captain
6 Gawlik and Gunnery Sergeant Whalen, you said that all their testimony
7 was going to be about the classified documents and the impact. Well,
8 actually, they're not going to talk about impact, right, because
9 they're just going to be testifying on the merits, is that right?

10 (U) ATC1: Yes, sir.

11 (U) MJ: Okay, and that answers the question.

12 (U) As far as Appellate Exhibits XXX and XXXI, which was the
13 submission by a defense counsel under M.R.E. 505(h), does either side
14 have any additional evidence to present on this at this point? Trial
15 counsel?

16 (U) ATC1: No, Your Honor.

17 (U) MJ: Defense?

18 (U) DC: No, sir.

19 (U) MJ: Okay, I'll hear arguments then. Trial counsel, do
20 you need to be heard?

[REDACTED]

[REDACTED]

1 (U) ATC1: No, Your Honor. I believe that you have all the
2 evidence you need before you with the affidavit and the OCA
3 determination and Chief Gendron's determination that they're
4 classified, Your Honor, to close those portions that specifically
5 relate to that part of the trial.

6 (U) MJ: Okay, thank you. Defense counsel?

7 (U) DC: Yes, sir. And sir, do you want me to go through
8 individually each of the----

9 (U) MJ: No, I'll do that, and just track along and make sure
10 I cover it adequately when I go through it.

11 (U) DC: Yes, sir. With regards to the matters that were
12 presented in the 505 notice, we would argue that we don't have any
13 objection, there were certain portions that we went through during
14 the 802 conference between the redacted and the unredacted portions
15 of Appellate Exhibit XXX and XXXI. We believe that for the majority
16 of the issues that we want to get across to the court, the unredacted
17 version of the 317 pages of emails is sufficient with the exception
18 of the specific emails that were pulled out and discussed during the
19 802 session. And we are amenable to having those things and we agree
20 that those things should be covered in a closed session because of

[REDACTED]

[REDACTED] [REDACTED]

1 the nature of the materials that are contained within those emails
2 and the things that will be discussed.

3 (U) MJ: Okay.

4 (U) DC: Sir, with regards to some of the other matters that
5 were listed in our 505 notice in regards to the ICRC reports and
6 those other things, those are still pending. I believe we're going
7 to do those on Monday. So, I'm just focusing this specifically on
8 the emails that were in the redacted and unredacted portions.
9 Specifically, Your Honor, we don't intend to introduce into evidence
10 those specific emails subject to the need for cross-examination or
11 impeachment or things of that nature, but those are emails that the
12 witnesses that we're going to present on direct examination and also
13 through cross-examination, that's information that will be touched
14 through cross-examination and direct examination. And so, those
15 emails are a representative sample of the nature of the information
16 that we want to get into. And so, those portions specifically
17 delineated for a closed session are those topics of information that
18 we believe should be closed to the public based on the nature of the
19 information.

20 (U) MJ: All right, thank you.

[REDACTED]



1 (U) Appellate Exhibits XXX and XXXI contain numerous emails,
2 attachments, memoranda, letters and similar documents. As the
3 defense counsel just stated, the defense does not intend to offer all
4 those documents during the trial but it was an intent to reduce to
5 writing the information they intended to elicit, either during cross-
6 examination or direct examination of witnesses. And I think it was
7 helpful in that regard; it was easier to see it in context with
8 everything else and it enabled the government to process that up
9 through the original classification authority who went through it in
10 great detail and delineated which parts were classified and which
11 were not. So I think that was helpful in getting that accomplished.

12 (U) I find that certain information within those exhibits,
13 specifically in four general areas, and they've been redacted out of
14 Appellate Exhibit XXXI, are classified as "secret" by the proper
15 original classification authority which is the Commander of the
16 Multi-National Force, Iraq, which is currently General Petraeus, in
17 accordance with Executive Order 12958 as currently amended. The four
18 general topics are JIDC incentives, detainee and family names,
19 manning issues and weaknesses and the intelligence collection,
20 including methods and procedures. Those four very broad subjects



[REDACTED]

1 fall within the categories in sections 1.4 Alpha, Charlie and Delta
2 of Executive Order 12958.

3 (U) Also, and more specifically, upon comparing the redacted and
4 unredacted copies of the materials that the defense had submitted
5 under Military Rule of Evidence 505(h) notice, the defense pinpointed
6 specific facts that were redacted that it wants to elicit in a closed
7 session. Those facts are...and I boiled it down to 15 that I think
8 adequately covers what the defense wants to cover.

9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 (U) Second, details on detainee privileges covering phone calls
13 and visits.

14 [REDACTED]
15 [REDACTED]
16 (U) Fourth, ICRC issues; and we'll address that later as far as
17 ICRC issues.

18 [REDACTED]
19 [REDACTED]

[REDACTED]

[REDACTED]

1 [REDACTED]

2 [REDACTED]

3 [REDACTED]

4 (U) Seventh, more information about the release procedures.

5 (U) Eighth, the fact that third country nationals are detained
6 at Camp Cropper.

7 (U) Ninth, a specific 510 request for Detainee Number 184.

8 (U) Tenth, an increase in the number of family visits and phone
9 calls over a certain period of time as shown with the chart.

10 (U) Eleventh, more information concerning the ICRC, specifically
11 their reports.

12 [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 (U) And fifteenth, information on the mission of Camp Cropper,
19 why it was designed and what its current mission is now.

20 (U) Defense counsel, have I adequately covered the points that
21 you brought up?

[REDACTED]



1 (U) DC: Yes, sir.

2 (U) MJ: I think you had it down to 19 or so, but I think some
3 of them were redundant.

4 (U) DC: Yes, sir.

5 (U) MJ: I find that this specific information is classified
6 "secret" by the proper original classification authority in
7 accordance with Executive Order 12958 as currently amended. And this
8 specific information does fall within the categories and sections
9 1.4(a), (c) and (d) of Executive Order 12958. From all the evidence
10 and from the circumstances in this particular case...now, before I
11 state this, let me clarify. I said earlier we were going to handle
12 the ICRC information separately. So, there were two of the 15 items
13 that mentioned the ICRC, so this ruling does not apply to those.
14 Those will be handled separately. For the other 13 items and also
15 for the four general categories mentioned in the affidavit, I am
16 satisfied that there is a reasonable danger that presentation of
17 these materials before the public in open court will expose military
18 matters which in the interest of national security should not be
19 divulged. Also, the danger is of significant--well, correction, is
20 of sufficient magnitude to outweigh the interest in having all trials
21 open to the public.



[REDACTED]

1 (U) Now defense counsel, are you able to delineate which witness
2 is going to talk about any of these specific matters, or is it going
3 to depend on the direct examination?

4 (U) DC: Sir, a majority of it will depend on the direct
5 examination because both defense witnesses and government witnesses
6 in a lot of circumstances will cross. And so, the information we
7 need to get out from those witnesses we put on our witness list will
8 likely come through cross-examination as opposed to calling them
9 again during the defense's case.

10 (U) MJ: Understood. Trial counsel, does the government
11 intend to go into any of these areas on direct examination?

12 (U) ATC1: One moment, Your Honor. [Pause.] Sir?

13 (U) MJ: Yes.

14 (U) ATC1: I think there's a little bit of clarification--I'd
15 ask for a little clarification on your ruling on detainee privileges.

16 (U) MJ: Yeah, I said details on detainee privileges. So
17 there, it would be...and it's hard to articulate. What's clear in

18 Appellate Exhibits XXX and XXXI is the general nature of detainee
19 privileges is not classified. But when you get into the specific
20 details of how many calls are allowed, how long someone has to be
21 there before they're authorized to call. So really when I say that,

[REDACTED]

[REDACTED]

1 I'm talking about the redacted portions within Appellate Exhibits XXX
2 and XXXI. That's what's classified "secret," so that's what I'm
3 wondering is whether you're going to go into any of those details
4 with any of your witnesses. Is it unclear at this point?

5 (U) ATCl: No, sir, I believe we will on several witnesses get
6 into the specific phone calls that detainees are allowed and how
7 we're alleging that Colonel Steele deviated from that when he
8 provided an unmonitored phone call. So, to the extent--I believe,
9 Your Honor, that it's either going to be covered by 506 as we made
10 that request when that comes in, and depending on--I think the
11 specificity is if it's tied to a specific detainee, that's when it
12 becomes classified. If it's not tied to a specific detainee....

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1
2
3
4
5
6
7
8
9
10
11

12 (U) ATCl: Yes, sir, I can give you a list of government
13 witnesses that are going to touch on that area, sir?

14 (U) MJ: Sure, please.

15 [REDACTED]
16 [REDACTED]
17 [REDACTED]

18 [REDACTED]
19 [REDACTED]

20 (U) MJ: And defense counsel, are you able to add any to that
21 list?

[REDACTED]

[REDACTED]

1 (U) DC: Yes, sir. Sir, Sergeant Major Winkleman, who was
2 Colonel Steele's sergeant major in that time. He'll probably touch
3 on issues like the mission of Camp Cropper, the persons at Camp
4 Cropper...oh, I'm sorry, did you just want the names, sir?

5 (U) MJ: Yes, just the names.

6 (U) DC: Sergeant Major Winkelman, probably Lieutenant Colonel
7 Vartanian, Staff Sergeant Findley and Captain Merritt. And then,
8 sir, from the government's list, we believe that those soldiers that
9 served as guards or Sally Port guards or things of that nature that
10 may be testifying about specifics will also get into some of those
11 things during cross-examination or it may come out through direct.

12 (U) MJ: Okay, all right, that's sufficient. Okay, so for
13 those witnesses...and counsel, I'll be tracking, if you're not
14 following, be sure I'll correct you on the spot. But what I need you
15 to do is like I said, package your classified and unclassified. And
16 the reason why that's important, twofold; one, is I don't want to
17 close the court and then have a lot of unclassified information
18 coming out when I could have had the public sitting in here listening
19 to all that. I don't want that. And then second, for judicial
20 economy, I don't want this to be a parade in and out of the courtroom
21 all day long during one witness' testimony. So those are my two

[REDACTED]

[REDACTED]

1 purposes for having you package it. So I think everyone's clear on
2 that and if I think you're not doing that, I'll just correct you on
3 the spot.

4 (U) Okay, next, we're going to talk about two specific areas
5 that were within those same two appellate exhibits, XXX and XXXI.
6 They went up to different original classification authorities and the
7 two issues are, one is a letter from Ambassador Khalilzad to the
8 Prime Minister of Iraq, and also I think there was a memo to the
9 Ambassador from one of his employees concerning the same letter. And
10 then also, there's a request from the Commander of Task Force 515 to
11 the Commander of Task Force 134 concerning incentive approach
12 techniques. I just want to approach those separately because they
13 did go up to a different OCA.

14 (U) Do counsel for either side need to be heard on either of
15 these two separate documents?

16 (U) ATCl: No, Your Honor.

17 (U) DC: No, sir.

18 (U) MJ: Okay, and first of all, I think I had mentioned
19 earlier that at the back of Appellate Exhibit XXXIV was added a
20 department notice from the Department of State. It concerns whether
21 or not a certain position was authorized or delegated the authority

[REDACTED]

[REDACTED]

1 of original classification authority. And looking at that document,
2 it does address the issue I had. On the bottom of the third page,
3 top of the fourth page, it specifically addresses that. And the
4 document this appellate exhibit is talking about is a letter from the
5 Ambassador to the Prime Minister of Iraq; it's dated 5 January 2006
6 and it's also an action memo to the Ambassador from his employee, Mr.
7 David Litt, and that's dated 11 October 2005. There's a letter and
8 memo that discusses the international and coalition implications of
9 the release of two HVDs in January of 2006. The HVDs are mentioned
10 by name and discuss the quantum of evidence in their criminal cases.

11 (U) This document has been classified as "secret" by the proper
12 original classification authority, which is the section head of the
13 Political Military Affairs at the U.S. Embassy in Iraq, who at the
14 time was Ms. Karen Sassahara, in accordance with Executive Order
15 12958 as currently amended. And the information within that letter
16 does fall within the categories in sections 1.4(b) and 1.4(d). From
17 the evidence and the circumstances in this case, I am satisfied there
18 is a reasonable danger that presentation of these materials before
19 the public in open court will expose military matters which in the
20 interest of national security should not be divulged and that danger
21 is of sufficient magnitude to warrant closing the court.

[REDACTED]

[REDACTED]

1 (U) Now defense counsel, what's the means by which you're going
2 to elicit that information, the actual letter or just through
3 testimony?

4 (U) DC: Sir, just testimony.

5 (U) MJ: Okay, and then just handle that testimony the same
6 way as the other areas that we just discussed.

7 (U) DC: Yes, sir.

8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]

[REDACTED]

1
2
3
4
5

6 (U) Defense counsel, again, the same question, do you intend to
7 offer that document or is it through a testimony of witnesses?

8 (U) DC: It's just through the testimony of witnesses, Your
9 Honor.

10 (U) MJ: Okay, handle that the same way I directed the other
11 information.

12 (U) Counsel, now what we're going to do is we're going to
13 address the information that's contained in Appellate Exhibit XXIX.
14 The information that I just covered also was covered by Appellate
15 Exhibit XXIX but we're going to cover the rest of the information
16 within there. Do counsel for either side have any evidence to offer
17 or arguments? Trial counsel?

18 (U) ATCl: Sir, just on the series of rules of engagement, both
19 MNF-I and MNC-I that are in that, that will likely...depending on how
20 you rule on the judicial notice, be documentary evidence. Otherwise,

[REDACTED]

1 we'll have to call a witness that will come in through testimony and
2 then as a document. So I just wanted to----

3 (U) MJ: I understand, sure. Fair enough; okay, that's
4 helpful.

5 Defense counsel?

6 (U) DC: Sir, can I briefly look at it?

7 (U) MJ: Sure. [DC reviews exhibit.]

8 (U) DC: Sir, are we talking to Binder 1, those documents in
9 Binder 1?

10 (U) MJ: Yes, all the documents in Appellate Exhibit XXIX,
11 there should be 11. Have you had a chance to look at that?

12 (U) DC: Yes, sir, with the exception of tab 1, but the other
13 ten tabs, we have.

14 (U) MJ: Go ahead and look at tab 1, then. And apparently,
15 trial counsel, you can correct me if I'm wrong, but it will help the
16 defense counsel, it appears that tab 1 was evidence you intend to
17 elicit from witnesses through witness testimony. And apparently, it
18 appears that someone went through and put in red all the testimony
19 that would be "secret," classified as "secret". And then when it
20 went up for the OCA determination, it was determined that that red
21 testimony is "secret," is that correct?

[REDACTED]



1 (U) ATC1: One moment, Your Honor.

2 (U) MJ: Sure.

3 (U) DC: Sir, with regards to some of the documents that are
4 in binder 1, I believe some of those SOPs are still pending review.
5 So, we may have more argument on those SOPs when we do that on
6 Monday.

7 (U) MJ: That's a good point. And we can talk about that now,
8 is I'm inclined at this point to find that tabs 2 through 5 have not
9 been classified by any authority, so they would not fall within
10 Military Rule of Evidence 505. So I'd either make that ruling or
11 what we could do is put that off. I think the trial counsel was
12 still working on that issue, whether they would fall under 506 or
13 some other rule.

14 (U) ATC1: Yes, Your Honor.

15 (U) MJ: So what I'll do is for tabs 2 through 5, I'll just
16 defer on those documents. So we're looking at 1 and 6 through 11;
17 that's a good point, defense counsel.

18 (U) DC: And sir, we're just specifically talking about the
19 closing of the hearing for discussion on those materials?

20 (U) MJ: Yes.



[REDACTED]

1 (U) DC: Yes, sir. Other than that, we don't have any other
2 argument for purposes of those enclosures or those tabs.

3 (U) MJ: First of all, I'm going to cover tabs 6 through 10;
4 I'm going to address them together. Those five tabs, the information
5 in those five tabs has been classified as "secret" by the proper
6 original classification authority, which is the Commander of the
7 Multi-National Force, Iraq, General Petraeus, and in accordance with
8 Executive Order 12958 as amended most recently on 25 March 2003.
9 Specifically, what's contained in those tabs is Multi-National Force,
10 Iraq, Framework Operations Order, dated 1 May 2006, marked as
11 "secret" overall with most portions marked "secret" and some marked
12 "unclassified". It contains the situation, mission, execution,
13 service support and command and signal. Tab 7 has Appendix 7 to
14 Annex C to MNC-I Operations Order 06-01, dated 21 April 2006. Also
15 marked as "secret" overall with most portions marked "secret" and
16 some marked "unclassified". This appendix contains the rules of
17 engagement for U.S. forces for OPORD 06-01. Tab 8 contains Appendix
18 4 to Annex C to Multi-National Corps, Iraq, Operations Order 05-02,
19 dated 27 July 2005, also marked as "secret" overall with most
20 portions as "secret" and some marked as "unclassified". This
21 appendix contains rules of engagement for U.S. forces. Tab 9

[REDACTED]



1 contains Appendix 5 to Annex C to Multi-National Force Framework,
2 Operations Order dated 1 May 2006, marked as "secret" with most
3 portions marked "secret" and some portions marked "unclassified".
4 This appendix contains rules of engagement for U.S. forces. And tab
5 10 contains tab Bravo to Appendix 5 to Annex C to Multi-National
6 Force, Iraq, Framework Operations Order dated 1 May 2006, marked as
7 "secret" overall with most portions marked "secret" and some marked
8 "unclassified". This annex contains definitions for rules of
9 engagement.

10 (U) From all the evidence and from the circumstances in this
11 case, I am satisfied that there is a reasonable danger that
12 presentation of these materials before the public will expose
13 military matters which, in the interest of national security, should
14 not be divulged.

15 (U) Next, I want to address tab 11, and that was a Military Rule
16 of Evidence 505 notice from the defense, dated 3 September 2007. It
17 was not marked as classified and the memo goes through in the

18 subparagraphs, in subparagraphs A through R talks about evidence that
19 may be offered at trial that could fall within Military Rule of
20 Evidence 505. I find that the information mentioned in subparagraphs
21 3e, 3f, 3g, 3h, 3i, 3k, 3l, 3n and 3r is classified as "secret" by



[REDACTED]

1 the proper original classification authority, which is the Commander
2 of Multi-National Force, Iraq, in accordance with Executive Order
3 12958 as amended. Now, as far as which categories within the
4 executive order it falls, I'll cover those separately. Subparagraphs
5 3d and 3f is classified "secret" as far as detainee names. And that
6 would fall within section 1.4(a) for military operations.
7 Subparagraph 3g talks about a roster of released detainees, and that
8 would fall within categories 1.4(a) for military operations and
9 1.7(e). And the reason for it falling within category 1.7(e) is
10 although individual facts within there might not be classified, the
11 compilation of the individual unclassified information meets the
12 requirement for a classification level of "secret".

13

14

15

16

17

18

19

20

21

1
2
3
4

5 (U) DC: Yes, sir.

6 (U) MJ: I'll still address it in hopes that they do testify.
7 But that information would fall within categories 1.4(a) and 1.4(c).
8 From the evidence, I find that the information in the subparagraphs I
9 just mentioned does create a reasonable danger that presentation of
10 these materials before the public in open court would expose military
11 matters which in the interest of national security should not be
12 divulged.

13 (U) Now, as far as the other subparagraphs, just so we're clear
14 on this, trial counsel, subparagraphs 3a through 3d, it doesn't fall
15 within Military Rule of Evidence 505, is the government pursuing a
16 different avenue of approach for those?

17 (U) ATC2: Yes, Your Honor, we're pursuing M.R.E. 506. We
18 believe, and I believe we marked it previously, but the memo signed
19 by the Secretary of Defense should be sufficient for that invocation,
20 because it does not apply to that specific case but to ICRC
21 communications generally, Your Honor.

[REDACTED]

1 (U) MJ: What we're going to do, what I intend to do is,
2 defense counsel, you haven't had a chance to look at that memo at
3 length, have you?

4 (U) DC: No, sir.

5 (U) MJ: And so obviously we're not doing trial by ambush, so
6 I'm going to give the defense counsel enough time to look at that and
7 then we'll litigate it when they've had ample opportunity to prepare.
8 Okay, so that's your approach with that one.

9 (U) And subparagraph 3j and 3m?

10 (U) ATC1: With regards to 3j, Your Honor, I believe that Chief
11 Gendron recommended that it be unclassified as stated. And now
12 specifics in specific cases will probably have to be treated
13 differently, Your Honor.

14 (U) MJ: So you're talking about specific detainee records, is
15 that it?

16 (U) ATC2: Yes, Your Honor, on j there. I think as stated, as
17 they stated, it's unclassified; however, I think it would be a
18 different case with more specific information.

19 (U) MJ: Okay, right, I'm looking at it. Defense counsel, do
20 you intend to get into specific detainee records or just the general
21 nature of the conversation that took place in the emails?

[REDACTED]

[REDACTED]

1 (U) DC: Sir, for j, that was the general nature. However,
2 it's also covered by subparagraph 3e, and those are the specific
3 records dealing with certain determinations of detainees. So 3e was
4 determined to be "secret," but in terms of the general information
5 and the classification level in general, that's testimony that would
6 be elicited but not necessarily specific to a specific detainee.

7 (U) MJ: Okay, you're right, yeah, because "e" was secret if
8 it got into a specific detainee with the name.

9 (U) DC: Yes, sir.

10 (U) MJ: Okay, understood, all right.

11 (U) ATC1: Sir, Your Honor, to the extent that "e" and "j" are
12 redundant, if they don't get into any specifics, the government won't
13 have any issues with that.

14 (U) MJ: And, 3m?

15 (U) ATC1: Your Honor, again, this is a 506 request that's with
16 the Secretary of the Army that we hope to have signed before Monday,
17 Your Honor. You also did make a specific ruling a moment ago about
18 specific privileges as contained in those emails, Your Honor. So, a
19 portion of that obviously will be classified as you previously
20 determined and then a portion will hopefully as--on Monday, the 506
21 material.

[REDACTED]

[REDACTED]

1 (U) MJ: Is there any ambiguity as far as, what do I mean by
2 specifics concerning privileges or what's not specifics, it's easy.
3 All you have to do is if you look in and compare the redacted and
4 unredacted versions of Appellate Exhibits XXX and XXXI, you can see
5 the level of detail that's classified and the level of detail that's
6 not classified. So in my mind, there's a clear line there of what's
7 classified and what's not classified. All right, so you're saying
8 you hope to have a document from Washington concerning M.R.E. 506 by
9 Monday?

10 (U) ATC1: Yes, Your Honor.

11 (U) MJ: And subparagraph 3o does not appear to be classified
12 and it doesn't appear that there's any...it can be discussed in open
13 court. Is that right, trial counsel?

14 (U) ATC2: Well, again, Your Honor, I think there's a
15 distinction that the fact that we do segregate people, in general, is
16 not classified, Your Honor, but a specific case, again, you know, for
17 instance, "We segregated high value detainee number such and such
18 over here because of this specific reason," we probably crossed that
19 line. But again, as written here, that is not classified. The fact
20 that we do segregate people, itself, is not classified, Your Honor.

[REDACTED]

[REDACTED]

1 (U) MJ: Is that where you're going, defense counsel, is just
2 in general terms?

3 (U) DC: Just in general terms, yes, sir.

4 (U) MJ: Okay, all right, that's fine. Then that one should
5 be clear to discuss in the open then.

6 (U) Okay, 3p has already been covered by some of the other
7 rulings, I think, is that right, defense counsel? There's a couple
8 of things in there as far as....

9 [REDACTED]

10 [REDACTED]

11 [REDACTED]

12 (U) MJ: Exactly.

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 (U) MJ: Okay, that's the way I interpret it, too.

17 (U) 3q covers ICRC evaluations; that's going to be covered

18 separately when we discuss ICRC, and that will be Monday just because
19 defense needs time to prepare for that. And I think that covers all
20 of tab 11.

[REDACTED]

[REDACTED]

1 (U) Next, the only other tab we have left in the book, remember,
2 we're going to push tabs 2 through 5 off, is tab 1. Now, what that
3 is is the witness expected testimony. It's undated and what's
4 happened is someone has gone in there and put in red font specific
5 testimony. And then what's happened is when it went up to the OCA,
6 the OCA classified that testimony as "secret," which actually is the
7 way it works so it's clear as far as that testimony that the
8 government intends to elicit from those witnesses and those areas
9 would be classified as "secret".

10 (U) Does counsel for either side want to be heard on that tab,
11 tab 1?

12 (U) ATC1: No, Your Honor.

13 (U) MJ: Defense?

14 (U) DC: No, sir.

15 (U) MJ: I find that the synopsis of those 18 witnesses'
16 testimony, which is highlighted in red font, has been classified as
17 "secret" by the proper original classification authority, which is
18 the Commander of the Multi-National Force, Iraq, currently General
19 Petraeus, in accordance with Executive Order 12958 as amended. From
20 all the evidence and all the circumstances, I'm satisfied there's a
21 reasonable danger that the presentation of these materials before the

[REDACTED]

[REDACTED]

1 public will expose military matters, which in the interest of
2 national security, should not be divulged.

3 (U) I think we're almost there. We're going to next address
4 Prosecution Exhibit 1 for identification, which apparently contains
5 detainee records. Do counsel for either side have any evidence or
6 argument on this issue? Trial counsel?

7 (U) ATC1: Your Honor, I'm sorry, what binder are we talking
8 about again?

9 (U) MJ: It's PE 1 for ID; it's the detainee records, 15
10 detainees, computer printouts.

11 (U) ATC1: No, nothing from the government, Your Honor.

12 (U) MJ: Defense counsel?

13 (U) DC: Sir, not with regards to, I guess, the classification
14 levels. We're still reserving the same objection as before as to how
15 this evidence would actually come in during the court-martial.

16 (U) MJ: Understood, okay, yes, and we're just covering
17 Military Rule of Evidence 505 issues now.

18 (U) DC: Yes, sir.

19 (U) MJ: So I won't be admitting this document at this point.
20 So all normal evidentiary objections are still available to you.
21 Prosecution Exhibit 1 for identification contains Task Force 134

[REDACTED]

[REDACTED]

1 detainee records. It's undated; it's marked as "secret" and it has
2 printouts from a computer database that lists 15 detainee by ISN,
3 name, gender, nationality and current disposition. It has been
4 classified as "secret" by the proper original classification
5 authority, which is the Commander of Multi-National Force, Iraq,
6 General Petraeus and in accordance with Executive Order 12958 as
7 amended on 25 March 2003. This evidence does fall within the
8 categories in sections 1.4(a) and 1.4(c). From all the evidence and
9 from the circumstances in this case, there is a reasonable danger
10 that the presentation of these materials before the public will
11 expose military matters, which in the interest of national security,
12 should not be divulged. It would hinder current military operations
13 by providing anti-Coalition members with a comprehensive list of
14 detainees which could also limit their value as sources. Also, it
15 provides details on the procedures of detainee operations, which
16 would hinder intelligence collection from future detainees. I find
17 that the need to exclude the public is of sufficient magnitude such
18 as to outweigh the danger of a miscarriage of justice which might
19 attend judicial proceedings carried out even in partial secrecy.
20 (U) Now trial counsel, how are you going to offer this? It's
21 going to be offered as a document, is that correct?

[REDACTED]

[REDACTED]

1 (U) ATC1: 902(11) notice, we provided that to the defense, yes,
2 803(6), Your Honor. Not through witness testimony, I guess is the
3 answer, Your Honor.

4 (U) MJ: Not through witness testimony. Well, I was just
5 looking at as far as how we're going to bifurcate the trial, but
6 we'll leave that up to just normal evidentiary objections.

7 (U) All right, so to summarize, I think we're done with the
8 Military Rule of Evidence 505 issues that we're going to address
9 today. The issues that are still open are there were some...well,
10 the issue about ICRC records and evaluations. Defense counsel is
11 going to get a chance to look at the memo from the Department of
12 Defense concerning that and then we'll discuss that Monday morning.
13 Also, there's some information that was covered today that has not
14 been classified as "secret". The defense counsel said they may be
15 getting something from Washington on that and we'll cover that on
16 Monday. Or, if there's some other argument on why that would be
17 covered in a closed session, we'll cover that on Monday.

18 (U) Counsel, what I want to do now is to litigate motions that
19 are still pending. Yes, trial counsel, you're standing up?

20 (U) ATC1: Your Honor, there was an additional portion, I guess
21 it's round three for a lack....

[REDACTED]

[REDACTED]

1 (U) MJ: Round three?

2 (U) ATC2: Round three, there was the database that we just
3 discussed, but the defense had also submitted detainee records.

4 (U) MJ: And has that been marked as an appellate exhibit?

5 (U) ATC1: I believe so, Your Honor. And Your Honor, the issue
6 there is that many of those or some of those documents were declared
7 classified by the OCA, but there are some in there that are not
8 classified. [Pause.] And Your Honor, not to complicate matters too
9 much, but...and I wish I'd brought this up at the 802 session, but we
10 also received the 902(11) notice from the defense yesterday with
11 documents similar to those but not included in that and have never
12 received a classification review, and there's I think 19 documents in
13 the 902(11) notice that have not been sent to the OCA.

14 (U) DC: Sir, if you look at the 505 notice, I believe that
15 those were actually already reviewed because both of those documents
16 that you're reviewing fall under 3 Echo and 3 Foxtrot and that 3 Echo
17 pertains to the various magistrate reviews, the Article 78 board
18 determinations conducted on the detainees linked to Charge I. And
19 subparagraph 3 Foxtrot, specifically pertains to...the documents
20 pertain to the release and approval for release of the detainees from
21 Camp Cropper from that period of time, and it specifically delineates

[REDACTED]

[REDACTED]

1 (U) MJ: And so if there's information here that's not secret,
2 it comes out in open court. Or are you pursuing an argument that it
3 falls within 506?

4 (U) ATC1: We believe it falls within 506, Your Honor. We sent
5 them to OTJAG; however, the likelihood of getting that to the
6 Secretary of the Army before Monday is extremely low.

7 (U) MJ: But did they go up with the other stuff that they
8 were going to the Secretary of the Army with?

9 (U) ATC1: No, Your Honor. I think there was over a thousand
10 documents within these detainee packets, 1,400 to be exact, and we
11 asked the defense to identify the specific documents and they did.
12 They gave it to us on 2 October. We got them up to OTJAG. The other
13 stuff that went to OTJAG, I can give you the exact date if you give
14 me a moment, Your Honor.

15 (U) MJ: Was it some time in September?

16 (U) ATC1: Yes, Your Honor.

17 (U) MJ: Well, what increases your chances of speed up there
18 is if they were already moving to get in front of the Secretary with
19 some other related documents, the chances that they might be able to
20 whip all that stuff together and bring it in at the same time is a
21 little better. So they may be able to get that in. This issue

[REDACTED]

[REDACTED]

1 appears to fall within the same issues that we're going to be
2 covering Monday. So we're just going to cover this area on Monday
3 when we address similar issues.

4 (U) But trial counsel, thank you for bringing that up. I had
5 overlooked that one binder.

6 (U) Counsel, what I want to do now is litigate two motions that
7 are pending. The first motion concerns a motion to dismiss by the
8 defense. Let me just ask before we go into an open session, does
9 anyone intend to present any, on this motion, any evidence in open
10 court? If it's a document, you can submit a document and it may be
11 classified and it will be handled appropriately. Does anybody intend
12 to present any testimonial evidence or argue concerning classified
13 information during this motion?

14 (U) ATC3: The government, sir, has classified information to
15 offer on behalf of the motion. There's a lot of unclassified
16 information, too, that the government is prepared to offer that will
17 confirm what the OCA declared as...the database printout that's been
18 marked "secret" and properly classified "secret". A lot of the
19 classified information will be presented based on the fact that we're
20 going to be talking about these allegations being at Camp Cropper,
21 these enemies being at Camp Cropper, which we'll verify that these

[REDACTED]

[REDACTED]

1 individuals were all at Camp Cropper at that time. So, the
2 government believes that most of its argument is going to be in a
3 classified setting, although some of the documents are mixed as
4 unclassified and classified.

5 (U) MJ: Sure, no, that's fine. But is part of your argument
6 you're going to have to talk about classified information?

7 (U) ATC3: About classified information, yes, sir.

8 (U) MJ: And defense counsel, you'll probably have to do the
9 same if they do that. So what we'll do then is we're going to open
10 up the court and when we get into that portion, we're just going
11 to...it's good practice for how the trial is going to run, is I'll
12 take the first argument by the proponent of the motion, whoever has
13 the burden of proof, and then go unclassified. And then when you're
14 ready to go into classified information, just ask for the court to be
15 closed. We'll go into closed session. And then when you're done,
16 we'll go to the opponent's argument, start with the classified since
17 it's already closed and when you're done with the classified
18 argument, then we'll open the court and then we'll go unclassified.
19 Is everyone clear on that?

[REDACTED]

[REDACTED]

1 (U) DC: Sir, I don't believe that the argument that we're
2 going to present is going to cover any classified materials. We're
3 just going to rely on the documents for review of the court.
4 (U) MJ: Okay, fair enough then. We're going to go into an
5 open session now. So, if someone could just let the bailiff know and
6 the bailiff can come in.
7 (U) We're going to take a recess in place. The court is in
8 recess.
9 (U) [The Article 39(a) session recessed at 1425, 12 October 2007.]

10 [END OF PAGE.]

[REDACTED]

Appellate Exhibit 511

Enclosure 3

69 pages

classified

"SECRET"

ordered sealed for Reason 2
and Reason 7 (government)

Military Judge's Seal Order
dated 20 August 2013

stored in the classified
supplement to the original
Record of Trial

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Government Targeted Brief
on Courtroom Closures

Enclosure 4

29 March 2013

Encl 4 to
APPELLATE EXHIBIT 511
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

UNCLASSIFIED

UNITED STATES OF AMERICA)	
)	Prosecution Motion To
v.)	Close Portions of the Court-Martial
)	For the Receipt of Classified
Anderson, Ryan G.)	Information
Specialist (E-4), U.S. Army)	
Headquarters and Headquarters Company)	6 July 2004
2122d Garrison Troop Support Brigade)	
Fort Lewis, Washington 98433)	

RELIEF SOUGHT

The Prosecution in the above case requests that the Court close those portions of the Court-Martial of Specialist Anderson for the receipt of classified information. The Prosecution requests oral argument.

BURDEN OF PROOF AND STANDARD OF PROOF

As the moving party, the Government bears the burden of proof. R.C.M. 905(c)(2). Additionally, the Government bears the burden of establishing a compelling need to close the proceedings that is narrowly tailored (United States v. Grunden, 2 M.J. 166 (CMA 1977) and U.S. v. Hershey, 20 M.J. 433 (CMA 1985)).

FACTS

On 6 October 2003, Specialist Ryan Anderson posted a message to a website called Brave Muslims.com. Brave Muslims.com is a website that caters to anti-American/pro-al Qaida sentiment. In that posting SPC Anderson stated that "Soon, very soon, I will have an opportunity to take my own end of the struggle against those who oppress us, to the next level", SPC Anderson then invited other members of Brave Muslims.com to contact him. Ms. Shannon RossMiller contacted SPC Anderson via electronic mail (email) using a false name. Ms. RossMiller is a member a private organization called Seven Seas which monitors the internet watching for possible terrorist threats. Ms. RossMiller corresponded with SPC Anderson via email between November and December 2003. In the correspondence with Ms. RossMiller, SPC Anderson stated he wished to switch sides or defect from the U.S. Army and join Muslim extremist forces fighting against the United States. Ms. RossMiller contacted the FBI and passed to them the information she had gathered regarding SPC Anderson.

In late 2003, the Federal Bureau of Investigation (FBI) began an investigation into SPC Anderson. As part of its investigation, the FBI contacted the Fort Lewis resident office of the U.S. Army Intelligence and Security Command (INSCOM). In January 2004, Army Counter Intelligence agents, posing as members of al Qaida, began corresponding with SPC Anderson via cell phone text messages. After a lengthy period of text messaging between Army Counter

UNCLASSIFIED

APPELLATE EXHIBIT X

UNCLASSIFIED

Intelligence and SPC Anderson, a meeting was arranged. On 9 February 2004, SPC Anderson met with an Army Counter Intelligence agent who claimed to be a member of a terrorist organization. After the first meeting a second meeting was arranged for the following day. The second meeting was conducted in a Government sport utility vehicle (SUV), which had been equipped with video and recording equipment. The second meeting, which lasted approximately an hour, was both recorded and videotaped.

During the text messaging and at the second meeting with Army Counter Intelligence personnel, SPC Anderson provided information regarding specific vulnerabilities of various weapons systems including the M1A1 and M1A2 Abrams Tank. The information provided by SPC Anderson was sent to the United States Army Tank Automotive and Armaments Command (TACOM) for a classification review. Approximately two lines of text messages sent by SPC Anderson and ten minutes of the videotaped meeting contained information which has been classified as secret by Brigadier General Roger A. Nadeau. General Nadeau is the original classification authority (OCA) for TACOM.

On 12 February 2004, the accused was apprehended, ordered into pretrial confinement, and charged. Following apprehension, INSCOM conducted a classification review of its investigative and related files. While the investigative file was declassified, two related files dealing with INSCOM undercover operatives underwent a classification review. As a result of that review, the commander of INSCOM, Major General John F. Kimmons, determined that information concerning the undercover operatives, as well as the means and methods of INSCOM undercover operations were classified secret.

LAW

Executive Order
E.O. 13292

Rules for Court Martial
R.C.M. 806(b)
R.C.M. 905(d)

Military Rule of Evidence
M.R.E. 505(i)
M.R.E. 505(j)

Case Law

U.S. v. Brown, 22 C.M.R. 41 (1956)

U.S. v. Grunden, 2 M.J. 116 (CMA 1977)

U.S. v. Hershey, 20 M.J. 433 (CMA 1985)

Globe Newspaper Co. v. Superior Court of Massachusetts, 457 U.S. 102 (1982)

Press-Enterprise Co. v. Superior Court of California, 464 U.S. 501 (1984)

UNCLASSIFIED

UNCLASSIFIED

WITNESSES/EVIDENCE

The Prosecution does not request any witnesses. The Prosecution requests that the Court consider the enclosures to this motion.

ARGUMENT

In accordance with the discussion section of R.C.M. 806(b), a court-martial may be closed without the consent of the accused when it is done in accordance with M.R.E. 505(j). M.R.E. 505(j)(5) authorizes a military judge to close a court-martial "during that portion of the presentation of evidence that discloses classified information." The analysis to M.R.E. 505(j) indicates that M.R.E. 505(j) is principally derived from U.S. v. Grunden and U.S. v. Hersey. Grunden and Hersey provide a framework for analyzing when, under the 1st and 6th Amendments, it is appropriate to close a court-martial. The Government's motion will first address the 6th Amendment and then the 1st Amendment.

The 6th Amendment to the United States Constitution states, in part, that "in all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial." Despite the language of the 6th Amendment, courts have long recognized that "the right to a public trial is not absolute." Grunden, at 120, also United States v. Brown, 22 C.M.R. 41 (1956). An accused's right to a public trial can give way in order to protect the identity of an undercover law enforcement officer, to preserve the orderly execution of a trial, and to receive classified information. Grunden, at 121 note 6.

In accordance with United States v. Grunden, before a court-martial can be closed the Government must demonstrate that closing the trial is necessary to prevent the disclosure of classified information. Additionally, the Government must narrowly tailor the closure to ensure public access to as much of the trial as possible without endangering classified information. The court in Grunden suggests that military judges conduct "a preliminary hearing which is closed to the public" to determine whether the Government has met its burden.

As enclosures to this motion the Government has provided a copy of declarations made by Major General John F. Kimmons and Brigadier General Roger A. Nadeau. Both General Kimmons and Nadeau are original classification authorities, authorized to classified information up to the secret level. The Government anticipates introducing the classified information described in General Nadeau's declaration in its case in chief. The classified evidence will include: approximately two lines of text message from SPC Anderson to Army Counter Intelligence agents; approximately ten minutes of a one hour videotape where SPC Anderson discusses classified information; six photos demonstrating damage done to M1A1 Abrams Tanks by a specific weapons system; and part of the testimony of one witness, Mr. John Rowe. Mr. Rowe will testify as to the truthfulness of statements made by SPC Anderson. It will be necessary to close the court-martial when Mr. Rowe testifies regarding the truthfulness of classified statements made by SPC Anderson. Mr. Rowe will also testify regarding the photos of damaged and destroyed M1A1 Abrams Tanks. The Government does not anticipate introducing any evidence regarding General Kimmons' declaration but requests that the court close the court-

UNCLASSIFIED

UNCLASSIFIED

martial during any cross examination conducted by defense counsel which delves into the areas described in General Kimmons' declaration.

Through the enclosed declarations, which have been made under penalty of perjury, the Government has established that the information contained in the declarations is classified. According to Executive Order 13292 which further amended Executive Order 12958, as Amended, Classified National Security Information, four prerequisites must be met in order to originally classify information:

- (1) An original classification authority is classifying the information;
- (2) The information is owned by, produced by or for, or is under the control of the United States Government;
- (3) The information falls within one or more of the categories of information listed in section 1.4 of this order; and
- (4) The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

Section 1.4 of Executive Order 13292 states:

Information shall not be considered classified unless it concerns:

- (a) military plans, weapons systems, or operations;
- (b) foreign government information;
- (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
- (d) foreign relations or foreign activities of the United States, including confidential sources;
- (e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;
- (f) United States Government programs for safeguarding nuclear materials or facilities;
- (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

UNCLASSIFIED

UNCLASSIFIED

(h) weapons of mass destruction.

Each of the four prerequisites for the classification of information is addressed in General Kimmons' and General Nadeau's declarations. As noted in United States v. Grunden, the "initial review by the trial judge is not for the purpose of conducting a de novo review of the propriety of a given classification decision. All that must be determined is that the material in question has been classified by the proper authority in accordance with the appropriate regulation. . . . The sole purpose of the review is to protect the accused right to a public trial by preventing circumvention of that right by the mere utterance of a conclusion or blanket acceptance of the government's position without the demonstration of a compelling need." Grunden at 123. The information contained in General Kimmons' and General Nadeau's declarations were properly classified in accordance with Executive Order 13292 by individuals authorized to classify information.

In addition to establishing that the information in question is classified, the Government must also narrowly tailor the closure of the court-martial to insure the public has access to as much of the proceedings as possible while still protecting national security. The Government intends to introduce all of its classified information in a single closed session. During that closed session witnesses who have already testified regarding unclassified information would then retake the witness stand to provide information regarding classified information. United States v. Grunden recommends this method of bifurcating witness testimony, stating "this bifurcated presentation of a given witness' testimony is the most satisfactory resolution of the competing needs for secrecy by the government, and for a public trial by the accused." Grunden at 123. As previously discussed, at trial the Government will seek to introduce the surveillance video from the second meeting, at least fifty minutes of which are unclassified. The Government has redacted the classified portions of the surveillance video to allow the public access to as much of the proceedings as possible. The Government would seek to close the court-martial for the classified portions of the surveillance video. Similarly, as the vast majority of the text message statements are unclassified, the public would be allowed access to the text messages with the exception of the two classified messages. The Government does not seek the closure of the entire trial against SPC Anderson or even the entire testimony of any of the Government's witnesses, rather the Government only seeks that the trial be closed for the receipt of classified information.

In addition to an accused's right to a public trial, the United States Supreme Court has stated that the public has a 1st Amendment right to be present at criminal trials. Globe Newspaper Co. v. Superior Court of Massachusetts, 457 U.S. 102 (1982) and Press-Enterprise Co. v. Superior Court of California, 464 U.S. 501 (1984). In United States v. Hershey, 20 M.J. 433 (1985) the Court of Military Appeals established that the Supreme Court's declaration regarding the public's right to be present at civilian criminal trials also applied to courts-martial. In Hershey the court described a four part test to determine whether the public could be excluded from a court-martial. The test described in Hershey was: (1) the party seeking closure must advance an overriding interest that is likely to be prejudiced (2) the closure must be narrowly tailored to protect that interest (3) the trial court must consider reasonable alternatives to closure, and (4) the court must make adequate findings supporting the closure to aid in review. Hershey at 436.


UNCLASSIFIED

UNCLASSIFIED

The first two prongs of the Hershey test are virtually the same as the test under Grunden. Thus, the Government relies on its argument above regarding the first two prongs under Hershey. The third prong under Hershey requires the court to consider reasonable alternatives to closing the court-martial. In the case at bar there are not reasonable alternatives to closing the court-martial. The evidence the Government intends to introduce is classified as secret. In accordance with Executive Order 13292, Sec. 1.2(a)(2) secret information is, by definition, information whose unauthorized disclosure "reasonably could be expected to cause serious damage to national security." The only way to avoid prejudicing an overriding Governmental interest is by closing the court-martial. The final prong requires the trial court to make adequate findings to support the closure to aid in appellate review. The Government suggests that in accordance with R.C.M. 905(d) the court make essential findings that state at a minimum that: the information that is the subject of this motion was properly classified by General Kimmons and General Nadeau; disclosure of the information would be harmful to national security; the court should describe what sessions of the court-martial will be closed; and there is no reasonable alternative to closing the court due to the classified nature of the evidence.

CONCLUSION

For the foregoing reasons, the Prosecution requests that the Court grant its motion to close the court-martial in United States v. Anderson for the receipt of classified information.



TIMOTHY C. MCDONNELL
MAJ, JA
Assistant Trial Counsel

2 ENCLS

1. Declaration of Major General F. Kimmons, dated 6 May 2004. CLASSIFIED
2. Declaration of Brigadier General Roger A. Nadeau, dated 29 June 2004. CLASSIFIED

UNCLASSIFIED

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Government Targeted Brief
on Courtroom Closures

Enclosure 5

29 March 2013

Encl 5 to
APPELLATE EXHIBIT 511
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

UNCLASSIFIED

UNITED STATES ARMY TRIAL JUDICIARY
FOURTH JUDICIAL CIRCUIT
FORT LEWIS, WASHINGTON

UNITED STATES

v.

SPC RYAN G. ANDERSON
US Army National Guard, 540-11-7564
A Co., 1/303 AR Reg
Fort Lewis, WA 98433

ORDER TO CLOSE CERTAIN
PROCEEDINGS

1. By written motion filed on 3 August 2004, the government requests that the court order the trial proceedings closed to the public only while certain sensitive information is being introduced or is the subject of examination or argument to ensure that the information specified in the government's motion is not disclosed to the public (Appellate Exhibit XIII). The defense filed a brief in opposition on 6 August 2004 (Appellate Exhibit XIV), arguing that the government failed to meet its heavy burden under the Sixth Amendment. Also, the government made an oral request for a similar order to close the proceedings during the introduction of classified evidence, the examination of witnesses regarding classified evidence, and if counsel use classified evidence or describe it during argument. The defense does not object to closure on a limited basis as necessary to protect classified information. A session under Article 39(a) UCMJ was held on this matter on 9 August 2004. The parties were given an opportunity to present evidence and make argument.

2. Findings of Fact

a. The government intends to introduce into evidence certain items of evidence that have been deemed classified. This information is not within the public domain.

b. As the detailed military judge, the undersigned reviewed the evidence *in camera* in the presence of the Court Security Officer, as well as the classification certification for the evidence.

c. My review of the evidence and the accompanying security classification declarations by Major General Kimmons and Brigadier General Nadeau show that the government proved by a preponderance that the evidence in the form of documents, photographs, and testimony sought to be introduced which has been marked as classified at the "Secret" level was properly classified by an authorized original classification authority applying the standards of Executive Order 12958, as amended by Executive Order 13292, and departmental regulations.

d. Public disclosure of the classified evidence in this case would harm the national security of the United States in the manner described in the declarations by Major General Kimmons and Brigadier General Nadeau. Specifically, disclosure of this information would enable an enemy or any other group or person to learn of specific vulnerabilities of critical US weapons systems that have not been made public, and would provide a means of defeating these US weapons systems now in use on the battlefield in Iraq and Afghanistan. Those

UNCLASSIFIED

APPELLATE EXHIBIT XXVIX

UNCLASSIFIED

weapons systems are manned by soldiers now in combat, whose lives would be at great risk should the information be disclosed to the public.

e. The classified information sought to be introduced is critical to the government's prosecution of this case. The purpose of the evidence is to prove that the means allegedly described by the accused to defeat US weapons systems to those he allegedly believed were agents of al Qaida were true.

f. Mr. Rene Gonzalez, a Department of Army expert on tactical wheeled vehicle survivability, testified on 9 August as to the sensitive information in the form of documents, photographs, and testimony for which the government seeks the closure order. This information was subjected to a classification review but was not classified. It is highly sensitive information about current vulnerabilities of the weapon system identified by Mr. Gonzalez during his testimony. This weapon system is a critical one on the battlefield in Iraq. Mr. Gonzalez described the Army's current efforts to resolve the vulnerabilities of this system to minimize future losses of US lives in combat theaters. While Mr. Gonzalez testified that some of the vulnerabilities are known by defense contractors who work in this area, the vulnerabilities have not been disclosed to the public.

g. As with the classified evidence, the sensitive information is critical to the government's prosecution of the case, and will serve the same purpose as that described in subparagraph e, above.

h. On 19 August 2004, the Acting Secretary of the Army invoked a claim of privilege under Military Rule of Evidence 506 with respect to the sensitive documents, photographs, and testimony described by Mr. Gonzalez and which the government intends to introduce at trial. The declaration of privilege covers the same evidence the government described as sensitive in its brief. The Acting Secretary of the Army is authorized as the agency head to invoke the privilege. Secretary Brownlee determined that public disclosure of the information would imperil the lives of soldiers and be detrimental to the public interest. His determination was based upon personal review of the sensitive evidence, legal advice from The Judge Advocate General, and a declaration of the risks of disclosure from the Deputy Commanding General, I Corps and Fort Lewis (App Ex XXV through XXVII). The invocation of the privilege satisfies the requirements for such an invocation under Military Rule of Evidence 506.

3. Discussion: Military Rule of Evidence 505 discusses the rule of privilege for government classified information. Military Rule of Evidence 506 is the rule of privilege for government information other than classified information. The category of evidence often described as "sensitive" is not covered by either rule, but is recognized as subject to protection in certain circumstances by case law (e.g., United States v. Hershey, 20M.J. 433 (C.M.A.1985)).

The accused enjoys the right to a public trial under the Sixth Amendment. The general public, including the media, has a qualified right under the First Amendment to attend criminal trials (Richmond Newspapers v. Virginia, 448 U.S. 555 (1980)). The right to a public trial is included in the Manual for Courts-Martial at Rule for Courts-Martial (RCM) 806. Case law interpreting the First and Sixth Amendments, and RCM 806, show that neither the accused's nor the public's right is absolute. A military judge may, if necessary, close portions of the trial proceedings to the public provided the government makes an adequate showing of necessity and the closing is tailored to minimize the closed sessions to the absolute minimum necessary (United States v. Grunden, 2 M.J.116 (C.M.A. 1977), and Rule for Courts-Martial 801).

UNCLASSIFIED

UNCLASSIFIED

To support a closed proceeding, the government must first make a compelling showing that closure is necessary to prevent disclosure of information which must be protected from public disclosure. Closure is only necessary when alternative means of presenting evidence are not available. The government discusses possible alternative means in its brief and makes a compelling argument why they would not work. For example, if the government is limited to showing a witness a classified or privileged exhibit but not able to discuss its contents in open court because spectators were present, that would deprive the trial counsel of a critical means of proof, and deprive the defense counsel, the members, and the military judge the opportunity to ask the witness questions about the exhibit. None of the matters for which protection has been claimed by the government can be used by the government without testimony. They are not self-explanatory or self-authenticating. There are no alternatives to protecting the classified and privileged information from public disclosure during trial except by excluding the public for very limited periods during the trial.

The court has carefully applied the balancing test described in Grunden and later military and federal cases in analyzing the government's request. Even though the defense did not object to closure of the trial during receipt of classified information, I have applied the balancing test nonetheless in analyzing whether the proceedings may be closed during receipt of classified and the sensitive information for which the privilege under MRE 506 has been invoked in order to protect the public's First Amendment right of access to courts-martial.

4. Conclusions of Law: Based upon the foregoing, I hereby conclude:

- a. The government has met its burden of proving that evidence in the form of documents, photographs, and testimony that has been properly classified and similar evidence that is the subject of a properly-invoked privilege under MRE 506, and which is also sensitive information, will be introduced at trial as evidence critical to the government's case-in-chief.
- b. The government has proven by a preponderance that there is a reasonable danger that presentation of these materials before the public will expose military matters which in the interest of national security should not be divulged (Grunden, 2 M.J. at 122).
- c. The government has delineated those portions of its case that involve these materials.

5. Order of the Court: The trial proceedings in the above-captioned case will be closed to spectators during the introduction of classified evidence, and evidence which was described as sensitive in the government's motion and for which the privilege under MRE 506 has been invoked. Closure will occur only during the portions of a witness's testimony in which it is reasonably expected that the protected exhibit or testimony will be displayed or discussed, when counsel will make direct reference to the contents of a protected exhibit or testimony during argument or in questioning any witness and cannot do so without discussing the testimony or evidence in open court, or when the military judge must discuss the exhibit or testimony on the record and cannot do so without disclosing the protected contents in open court. The proceedings will be reopened to the public at the earliest opportunity. Therefore, if a witness is to testify on both matters in which the public must be excluded and matters during which the public may be present,

UNCLASSIFIED

UNCLASSIFIED

trial counsel will conduct direct examination in a closed session on only the matters in which the public must be excluded, followed by cross-examination on those matters only in the closed session. Trial counsel will then conduct direct examination in open court of that witness on matters that are not subject to closure, followed by cross-examination in open court on the same matters. While this procedure may require counsel to depart from normal practice of complete direct examination of a witness prior to cross-examination, the manner directed in this order will not impede the fair administration of justice and will ensure that the proceedings are closed only as absolutely required. Counsel are further directed to notify the judge in advance before eliciting classified or privileged evidence in open court, or discussing same. Finally, trial and defense counsel will advise the military judge before arraignment as to which parts of the record and exhibits, including allied papers, should be the subject of a protective order in the record of trial.

DONE THIS 26TH DAY OF AUGUST 2004 AT THE FOURTH JUDICIAL CIRCUIT, FORT LEWIS, WA.

Debra L. Boudreau
DEBRA L. BOUDREAU
Colonel, JA
Chief Circuit Judge

UNCLASSIFIED

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Government Targeted Brief
on Courtroom Closures

Enclosure 6

29 March 2013

Encl 6 of
APPELLATE EXHIBIT 511
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

UNCLASSIFIED

DEPARTMENT OF THE NAVY
NAVY-MARINE CORPS TRIAL JUDICIARY
CENTRAL JUDICIAL CIRCUIT
GENERAL COURT-MARTIAL

UNITED STATES

v.

Matthew Diaz
LCDR, JAGC, USN

COURT ROOM PROTECTIVE
ORDER

11 MAY 2007

1. This ORDER supplements the Closure Order issued this date.
2. Pursuant to the findings and conclusions in this court's Closure Order, the court finds that an additional Protective Order is required to address the orderly and secure process of court proceedings in which classified information might be present and might be published or otherwise disclosed. This Protective Order is issued by the presiding military judge, acting under his supervisory authority to ensure a fair and expeditious trial, while protecting the national security interests of the United States and pursuant to M.R.E. 505. The procedures set forth in this Protective Order apply in addition to those previously set forth in the Protective Order and Protective Order Modification #1 (Appellate Exhibits IV and X), the terms of which are incorporated herein by reference.
3. In determining the protective measures required in this case, the court has carefully reviewed the physical environment in which proceedings in this case are to be held, the needs of the parties for access to classified information and the need for public access to this court-martial. The court has taken judicial notice of and fully considered the provisions of the Department of Navy Information Security Program (SECNAVINST 5510.36A of 6 October 2006 and M-5510.36 of June 2006). The court has balanced the national security needs and protective policies of governing regulations against the rights of the accused to present an adequate defense at a public trial, and the need for orderly proceedings.
4. The court concludes that the following requirements are fully protective of information classified at the SECRET level and that no lesser means than those set forth below would adequately safeguard the classified information at issue in this case. While more stringent measures could perhaps provide a larger margin for error, that additional caution would provide no additional actual security. As a result, more stringent measures such as prohibiting the presence of properly protected classified information in open sessions of court would be an unjustifiable limitation on the accused's right to present an adequate defense at a public trial and would impede the orderly proceedings in this case. The following protective procedures are, therefore, the least intrusive of the accused's rights as is possible under the circumstances and the implementation of these measures will reduce the number and duration of closed sessions.

UNCLASSIFIED

APPELLATE EXHIBIT 1XXX
PAGE 1 OF 4
APPENDED PAGE _____

5. By copy of this Protective Order, the CSO is directed to immediately inform the court of any change in circumstances that, in his opinion, necessitates a modification of the security posture in, or immediately adjacent to, Courtroom No. 1 during the proceedings in this case.

6. Presence of Classified Documents. Open sessions of court are conducted in an open courtroom environment in which personnel are permitted to be present that do not have appropriate clearances or access to classified information. Therefore, classified documents shall only be brought into an open session of court if that document is required for reference during that session. Since classified material will be used during some open sessions, the following requirements are ordered:

- Central Circuit local rules for decorum in the courtroom shall be affirmatively and strictly enforced during all sessions of court. All photographic, sound or video recording equipment, any other recording device, cell phones, and all other electronic communication devices, are prohibited from entering the courtroom. Pagers or other electronic devices that are not capable of recording or transmitting are permitted in the courtroom, but must be cleared for entry by the CSO and must be placed in silent mode.
- All classified documents must be in the control of properly cleared personnel at all times.
- Any person carrying classified information into an open session of court must first notify the CSO of the number of documents and classification level of any such documents.
- All classified documents must be properly marked in accordance with regulations governing the classified information contained in the document.
- Classified documents may be carried into the courtroom, but must be contained in a briefcase or closed folder.
- All classified documents must be protected by affixing thereto a classified document cover consistent with regulations governing the classification level.
- When not in active use at counsel table, the podium or witness stand, classified documents shall remain inside a closed briefcase or a closed opaque folder. When being used by counsel or a witness, the document must remain covered, except the cover may be raised as needed by counsel or a witness to see the document's content. However, when the cover is raised, the classified document must remain flat on counsel's table, the podium, or witness stand.
- The CSO shall ensure that no classified document in use during any open session is visible from the gallery. If necessary, gallery seating will be removed to a distance from the bar sufficient to prevent inadvertent disclosures by counsel during use of classified information at counsel table and sufficient to protect against any intentional attempt by a gallery member to gain visual access to classified information. If, in the opinion of the CSO, there is insufficient distance to ensure security of classified information at counsel table from persons in the gallery, the CSO shall immediately so inform the court.

UNCLASSIFIED

- If a classified document is referred to, offered into evidence, or otherwise utilized during an open session, it must remain under a protective cover sheet and may only be referred to by exhibit number, and, if necessary, by its classification level and the unclassified title of the document. No disclosure or discussion of classified material contained in any document is permitted during open sessions of court.
- At the conclusion of any open session of court during which classified information was present, the CSO will verify with the parties that all classified information is accounted for, secure, and properly removed from the courtroom. The parties are individually responsible for the proper handling and storage of classified material in their control.
- The CSO shall be present in the courtroom during all open and closed sessions of court. He shall ensure that there is a visual mechanism, such as a remotely activated signal light, by which to notify the military judge in the event the CSO detects that an inadvertent disclosure of classified information is imminent or has occurred.

7. Discussion of Classified Information. No classified discussion may occur during open sessions of court. If any party determines a discussion of classified information is necessary, that party shall request a recess or a closed session of court. The latter shall be requested in accordance with M.R.E. 505 and the prior orders of this court.

8. Closed Session Procedures.

a. In the event the presiding military judge directs a closed session, all persons not on the approved access list shall depart from the courtroom and the passageways immediately adjacent thereto. A recess will ordinarily be used to facilitate clearing the courtroom of unauthorized personnel. Thereafter, a sentry with a current copy of the access list will be posted at the main entrance to Courtroom No. 1. Under the supervision of the CSO, that sentry may admit only those persons presenting positive identification and who are listed on the access list. Other entrances to the courtroom will be secured from the inside, allowing emergency egress only. If other entrances cannot be so secured, additional sentries shall be posted to prevent access via these entrances. All personnel seeking admittance to the courtroom will be directed to the main entrance. No person may be permitted to loiter in the passageways immediately adjacent to Courtroom No. 1 during closed sessions unless that person is on the access list.

b. Prior to commencement of a close session, the CSO will verify that the unclassified recording system has been disabled by the court reporter.

c. Prior to commencement of a close session, the CSO will verify that all external audio and video feeds have been disabled and will provide an access list to the military judge and to counsel for both parties, which list will be inserted into the record.

d. In the event counsel or a witness requires the use of computer media to display classified information, the proponent counsel shall coordinate use of such media with the CSO, who must first authorize use of any electronic equipment inside the courtroom.

UNCLASSIFIED

APPELLATE EXHIBIT 1XXX
PAGE 3 OF 4
APPENDED PAGE _____

e. When satisfied that the actions set forth in paragraphs a. through c. are completed, the CSO shall inform the military judge that conditions for a closed session have been met. The military judge will then call the closed session to order.

f. At the conclusion of a closed session, the CSO will ensure that any classified electronic system, including media, is properly secured. He will also collect any notes made by the trial counsel and the military judge and review those notes for the presence of any classified information. If these notes contain classified information, the CSO shall have those notes properly secured or destroy the notes after consultation with the drafter. The CSO shall also make arrangements with the defense for the review and proper disposition of any classified defense notes. Finally, at the conclusion of a closed session, the CSO shall verify that all classified documents have been collected and secured as set forth above, that is, removed from the courtroom to proper storage, or placed inside briefcases or closed folders on counsel table. When all classified information is properly secured, the CSO shall advise the military judge that the courtroom is prepared for an open session.

g. At a recess of court prior to members' deliberations, the CSO shall inventory all classified exhibits that have been admitted into evidence and that are to be provided to the members during their closed session deliberations. During the open session prior to deliberations, the senior member shall be provided classified and unclassified exhibits and he will be the custodian of all exhibits used by the members in closed session. At the conclusion of deliberations and upon returning to an open session of court, the senior member will return all exhibits to the CSO, who shall inventory and verify that all classified material is accounted for and properly secured.

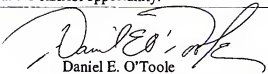
9. Storage of Classified Information.

a. The CSO has approved the storage of classified material by counsel in their local containers.

b. Storage of the original record of trial shall be stored in the safe labeled "Diaz Records" in Room B-204. Classified notes of the military judge shall be stored in this safe in a separate sealed envelope marked "Military Judge Notes." No other material may be stored in this safe without permission of the court.

c. The CSO will hold the combination to the safe labeled "Diaz Records" and will control access to it. The Region Legal Service Officer (RLSO) Security Manager will be provided the combination for use in an emergency, but, prior to opening the safe, the Security Manager must attempt to contact the CSO. In the event contact is not possible, the RLSO Security Manager must, as soon as possible, contact the CSO and report the nature of the emergency and any action taken. The CSO will inform the court at the earliest opportunity.

Entered this 11th Day of May 2007.


Daniel E. O'Toole
Captain, JAG Corps, U.S. Navy
Circuit Military Judge

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Government Targeted Brief
on Courtroom Closures

Enclosure 7

29 March 2013

Encl 7 to
APPELLATE EXHIBIT 511
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

UNCLASSIFIED

RECEIVED
CENTRAL
CIRCUIT

DEPARTMENT OF THE NAVY
GENERAL COURT-MARTIAL -8 JUN 07 12 35
NAVY AND MARINE CORPS TRIAL JUDICIARY
CENTRAL JUDICIAL CIRCUIT

UNITED STATES

v.

Matthew M. DIAZ
LCDR, JAGC, USN

GOVERNMENT MOTION FOR
APPROPRIATE RELIEF PURSUANT TO
MILITARY RULE OF EVIDENCE 505

1. Nature of Motion:

Pursuant to Rule for Court-Martial 906 and Military Rule of Evidence 505(e), the government moves for arraignment and a preliminary Article 39(a) session to consider matters relating to classified information that may arise in connection with the trial. Specifically, the government requests that the military judge issue a protective order under Military Rule of Evidence 505(g)(1) and establish timing for discovery and notice under Military Rule of Evidence 505(h). As the movant, the government has the burden to show that it is entitled to relief by preponderance of the evidence.

2. Facts:

In January of 2005, Ms. Barbara Olshansky received a card in an envelope bearing a return address at the Joint Task Force in Guantanamo Bay, Cuba. A determination was made that the information contained on the pieces of paper was and is classified at the SECRET/NOFORN level.

Subsequent investigation into the origins of the pieces of paper received by Ms. Olshansky determined that they contained information from the Joint Detainee Information Management System (JDIMS). This system is a classified web based computer program, which is accessible through the SECRET Internet Protocol Router Network (SIPERNET).

UNCLASSIFIED

APPELLATE EXHIBIT I
PAGE 1 OF 32
APPENDED PAGE 19

The convening authority referred charges in this case to a general court-martial on 5 January 2007. The information disclosed by the accused is still classified at the SECRET/NOFORN level.

3. Authority:

Military Rule of Evidence 505

4. Discussion:

The government moves pursuant to Mil. R. Evid. 505(e) for a preliminary session under Article 39(a) to consider matters relating to classified information that may arise in connection with the trial.

a. Pre-Trial Hearing

After referral of charges, "any party may move for a session under Article 39(a) to consider matters relating to classified information." Mil. R. Evid. 505(e). After such a motion, "the military judge promptly shall hold a session under Article 39(a) to establish the timing of requests for discovery, the provisions of notice under subdivision (h), and the initiation of the procedure under subdivision (i)." *Id.*

The government requests this hearing to establish defense notice requirements under Mil. R. Evid. 505(h) and a timeline for any proceedings that may be necessary under Mil. R. Evid. 505(i).

Mil. R. Evid. 505(h) requires that the defense provide the trial counsel notice if the defense reasonably expects to disclose or cause the disclosure of classified material in any manner during the court-martial process. The government requests this session so that the government can ensure that the proper documentation is obtained and requested in order that the courtroom can be properly closed for any defense requested disclosure for the purpose of protecting classified information.

Based on the inherent difficulty in dealing with classified information during the court-martial process, the government requests that this Article 39(a) session be held as soon as practicable to establish the requirements under Mil. R. Evid. 505(h) and 505(i).

b. Protective Order

The government also moves pursuant to Mil. R. Evid. 505(g)(1) for the issuance of a protective order to govern the handling of classified information in this case.

Mil. R. Evid. 505(g)(1) requires the court, upon the request of the government, to issue an order "to guard against the compromise of information disclosed to the accused." Mil. R. Evid. 505(g)(1) makes explicit the court's authority to issue protective orders for classified information. Mil. R. Evid. 505(g)(1) further provides that the protective order may include the following provisions:

- (1) prohibiting the disclosure of the information except as authorized by the military judge;
- (2) requiring storage of material in a manner appropriate for the level of classification assigned to the documents to be disclosed;
- (3) requiring controlled access to the material during normal business hours and at other times upon reasonable notice;
- (4) requiring all persons to cooperate with personnel in any investigations which are necessary to obtain a security clearance;
- (5) requiring the maintenance of logs recording access by all persons authorized by the military judge to have access to the classified information in connection with the preparation of the defense;
- (6) regulating the making and handling of notes taken from material containing classified information; and
- (7) requesting the convening authority authorize the assignment of government security personnel and the provision of government storage facilities.

A protective order issued by the military judge has the same force and effect as other orders issued by the military judge, and violations of a Mil. R. Evid. 505(g)(1) may be punished in the same manner that violations of other court orders are enforced.

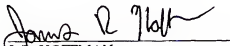
Here, the government seeks the issuance of a protective order seeking the terms set forth above, as well as other measures which it believes is necessary to protect the classified information at issue in this case. A proposed protective order is attached.

5. Attachments:

- a. Charge Sheet
- b. Affidavit of Mr. Paul Rester
- c. Proposed Protective Order

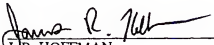
6. Oral Argument:

If this motion is opposed by the defense then the government requests oral argument.


J. R. HOFFMAN
DE JAGC, USN
Trial Counsel

CERTIFICATE OF SERVICE

I hereby certify that a copy of this response was served on Detailed Defense Counsel in the above captioned case on 8 January 2007.


J. R. HOFFMAN

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Government Targeted Brief
on Courtroom Closures

Enclosure 8

29 March 2013

Encl 8 to
APPELLATE EXHIBIT 511
PAGE REFERENCED: _____
PAGE OF _____ PAGES

GENERAL COURT-MARTIAL
UNITED STATES NAVY
SOUTHWEST JUDICIAL CIRCUIT
SAN DIEGO, CALIFORNIA

UNITED STATES)

3 May 2005

V.)

ORDER TO CLOSE CERTAIN
TRIAL PROCEEDINGS

ANDREW K. LEDFORD)
LT U.S. NAVY)

By written notice, the defense seeks to introduce classified information during closed sessions of this trial. By written motion, as amended orally during argument, the government requests that the court order the trial proceedings closed to the public only while certain classified information is being introduced or is the subject of examination or argument to ensure that the information specified in oral argument and in the attached appellate exhibits is not disclosed to the public. The defense does not object to closure on a limited basis as necessary to protect classified information. Two sessions under Article 39(a) were held on this matter. The parties were given the opportunity to present evidence and make argument.

Findings:

1. Both the government and the defense intend to introduce into evidence certain items that have been deemed classified. This information is not within the public domain. This evidence includes the names of protected-identity witnesses, the identity of participants in certain operations, and discussions or viewings of tactics/rolls/positions/locations, as well as the identification of the alleged victim. The defense additionally seeks to introduce classified information on sentencing that includes other direction actions in which the accused was involved, his current duties, the background of the alleged victim, and videos of other operations. This order addresses only the evidence to be offered on the merits. The court specifically withholds any ruling regarding evidence to be offered during presentencing to allow the parties to complete their preparations for presentencing.
2. Specifically, the government will seek to present to the members testimony from identity-protected witnesses, as well as testimony from or regarding witnesses whose mere presence on or association with particular missions is classified. The government does not object to this

being presented in closed session, but seeks to safeguard their identity from public view.

3. The government will also seek to offer into evidence the written statements allegedly made by the accused. While the government intended to offer redacted versions of the statements to avoid the presentation of classified passages from those documents, the defense desires that the entire statement be offered so that the members have the benefit of seeing the entire statement, and to avoid any speculation on the part of the members as to what might be missing from these documents. Although not specifically stated, the defense concern is that a limiting instruction from the court would not be sufficient to prevent prejudice to the accused. The government therefore seeks to offer the unredacted version of the statement, with the understanding that the classified portions will not be reference in open sessions. Neither party anticipates the need to discuss the classified contents of the statement in open court. Since members' questions will all be written, the court will have the benefit of knowing whether the members' question, if any, will necessitate a limited closed session of the court.
4. The defense will seek to introduce evidence regarding the positions, tactics, roles and activities of witnesses as those matters bear on ability to observe, ability to supervise, and the context in which some of the charged offenses occurred. In order to establish where certain witnesses were at particular times when events were observed, the defense may need to elicit classified information that would disclose, or at least permit a clear inference of, tactics, techniques and procedures of operational forces. They will also seek to introduce evidence regarding the positive identification of the alleged victim as it bears on the state of mind of the team members on the night in question and as it relates to establishing the identity of the named victim. Finally, because the government seeks to introduce a still photo from a video clip showing a prisoner wearing a mask that the government alleges amounts to mistreatment, the defense desires to offer entire video clip showing the capture of the prisoner so that the members can view the alleged offense in context. The entire video clip is less than 5 minutes long. The government does not object to this being presented in closed session, but seeks to safeguard these classified matters from public view because they will disclose classified tactics, techniques and procedures.
5. My review of the evidence and the accompanying security classification declarations show that the government has established by a preponderance of the evidence that the evidence in the form of documents, photographs, video and testimony sought to be introduced which has been marked as classified at the "confidential" and "secret" level was properly classified by an original classification authority applying

the standards of Executive Order 12958, as amended by Executive Order 13292, and various departmental regulations.

6. Public disclosure of the classified information in this case would harm the national security of the United States in the manner described within the declarations. Specifically, disclosure would reveal foreign government information, intelligence sources and methods, organization/functions/ names of agency employees, and the tactics/techniques/procedures of operations, and would thereby enable an enemy or other persons to learn specific vulnerabilities or otherwise impair future direct action missions of coalition forces.
7. The classified information sought to be introduced on the merits will tend to provide some evidence from which the members can determine the ability to perceive on the part of percipient witnesses, the extent and context of the witnesses' involvement in the charged offenses, and the identification of, and the ability of the accused to adequately supervise, subordinates on these missions.
8. The Secretary of the Navy and the Directory of Central Intelligence invoked the claim of privilege under Military Rule of Evidence 505 with regard to the same material the court has reviewed. Both the Secretary and the DCI are authorized as agency heads to invoke the privilege, and both have determined that disclosure of this material reasonably could result in damage to national security. Their determinations were based upon personal review of the evidence and declarations from subject matter experts. The invocation of the privilege satisfies the requirements of Mil.R.Evid. 505.

Conclusions:

1. The accused and the public enjoy the right to a public trial, but that right is not absolute. A military judge may, if necessary, close portions of the trial proceedings to public view if the government makes an adequate showing of necessity and the closure is tailored to limit the close sessions to the minimum necessary. *United States v. Grunden*, 2 M.J. 116 (C.M.A. 1977); Mil.R.Evid. 505.
2. To support a closed proceeding, the government must make a showing that closure is necessary to prevent public disclosure of information that must be protected. Closure is necessary when alternative means of presenting the evidence are not sufficient or available.
3. The court has carefully applied the balancing test described in *Grunden* and its progeny. Even though neither party objects to closure of the trial during receipt of classified information, I have applied the balancing test

nonetheless in analyzing whether the proceedings may be closed during the receipt of classified information.

4. The government has met its burden of establishing that the evidence at issue has been properly classified.
5. The government has met its burden of establishing that there is a reasonable danger that the presentation of these matters before the public will harm the national security.
6. The parties have delineated the subject matter that will involve classified information, and the subject matters are relevant, necessary and otherwise admissible.

Order of the Court:

1. The trial proceedings in this case will be closed to the public during the introduction of classified evidence. Closure will occur only during the portions of a witness' testimony in which it is reasonably expected that the protected exhibit or testimony will be displayed or discussed, or when counsel will make direct reference to the contents of the same during argument or in questioning, and cannot do so without discussing the testimony or evidence in open court. Closure will also occur when the military judge must discuss the exhibit or testimony on the record and cannot do so without disclosing the protected contents in open court. The proceedings will be reopened to the public at the earliest opportunity.
2. In addition to the preceding generalized order, the following specific orders apply:
 - a. The identity-protected witnesses shall testify behind a physical barrier that prevents the public from viewing the witnesses' physical appearance. However, the witnesses shall remain in the view of the members, counsel, the accused and the court at all times. The witnesses shall otherwise testify in open court, except during an initial closed session during which the witnesses' protected identity shall be established. All classified direct and cross-examination for identity protected witnesses shall be conducted during the initial closed sessions. The proceedings with thereafter be reopened to the public. No reference to the true names of these witnesses shall be made in open court. Counsel shall refer to them in open court with agreed upon pseudonyms.
 - b. Any references to specific missions that link particular individuals or particular agencies to those missions shall, if classified, be made in

closed sessions. Counsel shall thereafter refer to them in open court with agree upon pseudonyms.

- c. If a classified video footage is to be played for the members, video screens shall be adjusted so as to shield them from view of the public. Where possible, the court will remain open to the public during the playing of the video. Any classified testimony regarding the video, or classified portions of an audio track accompanying the video, shall be taken during closed sessions. The proceedings will thereafter be reopened to the public, shielding the screens from public view.
- d. Any classified document that can be offered in open session without addressing its classified contents shall be offered in open session.
- e. Any witness that shall testify in both classified and unclassified matters shall testify first during a closed session as to classified matters. The sponsoring counsel shall conduct a direct examination in a closed session on only the matters from which the public must be excluded. That examination will be immediately followed by a cross-examination and examination by the court on those same classified matters. Counsel and court will then conduct examination and cross-examination on matters not subject to closure in open court. While this procedure may force counsel to depart from normal practice, the manner directed will not impede the fair administration of justice and will ensure that the proceedings are closed only as absolutely required. If counsel desire to conduct the open session of examination and cross-examination first, with the closed session to follow, they shall notify the court.
- f. Counsel are instructed that they shall use alternative means of presenting evidence when available and acceptable to avoid the use of classified information. For example, if counsel intend to elicit testimony that at an agreed upon event, the witness passed a codeword signifying some relevant event, and the codeword is classified but the rest of the testimony is unclassified, counsel shall not elicit the classified codeword unless the codeword itself is necessary. Trial and defense counsel shall notify the court prior to opening statements precisely which witnesses they anticipate will require closed sessions. Counsel are further directed to notify the military judge in advance before eliciting classified evidence in open court, or discussing same.

- g. Counsel are instructed that they shall instruct their witnesses of the procedures to be used by the court. Witnesses shall be instructed by counsel that they are not to offer classified information while in an open, public session.

So ordered this 3rd day of May 2005.

C. L. REISMEIER
CDR, JAGC, USN
Military Judge

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

**Prosecution Objection to
Providing an "Example" Witness
to Examine the Viability of
Reasonable Alternatives to Closure**

3 April 2013

The United States respectfully objects to providing an "example" witness for the next Article 39(a) session to examine the viability of alternatives to closure. Based on the facts and circumstances of this case, an "example" witness would not assist the Court in testing whether alternatives short of closure are reasonable under Rule for Courts-Martial (RCM) 806. Examining whether alternatives are reasonable by way of an "example" witness would not be indicative as to whether alternatives are reasonable for the remaining witnesses and would only lead to frustration of judicial economy. To the contrary, there are no alternatives that are reasonable because those portions of testimony for which closure is sought are entirely and inextricably linked to classified information.

FACTS

On 31 January 2013, the United States requested courtroom closure, in whole or in part, for the testimony of 37 of the 141 government witnesses and provided the particular subject matter to which each witness would testify in a closed session. *See* Appellate Exhibit (AE) 479. The United States estimated that the requested closures comprised approximately 30% of its case.

On 1 March 2013, the Court ordered the United States to provide more specificity with respect to which portions of testimony closure was sought. *See* AE 503. In its supplemental response dated 15 March 2013, the United States provided a greater degree of specificity. *See* AE 505. Further, in light of reasonable alternatives available short of closure, the United States narrowed its list of witnesses for whose testimony closure was sought to 28. The United States requested courtroom closure for the entirety of four witnesses' testimony and for a limited portion of twenty-four witnesses' testimony. The United States currently estimates that the requested closures comprise approximately 25% of its case. *See id.*

On 28 March 2013, the defense argued that the United States must provide more specificity with respect to the classified information it intends to elicit from the 28 identified witnesses in order for this Court to consider all reasonable alternatives to closure. *See* Defense Request for Appropriate Relief: Closure Witness, dated 28 March 2013. The defense stated as follows:

[T]he only way to achieve the necessary level of specification is to actually hear the testimony of a witness delivered in a closed court session. Thereafter, while the Court remains closed, either party or

the Court may attempt to elicit the same information through the use of alternatives. Then, the Court will be in a better position to determine whether closure or use of an alternative is appropriate.

Id.

On 1 April 2013, the Court asked the United States whether it had any objection to providing an “example” witness for the next Article 39(a) session to examine the viability of alternatives to closure. Later that day, the United States stated its objection and requested an opportunity to file a written brief, which the Court granted.

WITNESSES/EVIDENCE

The United States requests the Court consider the enclosures to this filing and the Appellate Exhibits cited herein.

LEGAL AUTHORITY AND ARGUMENT

The United States respectfully objects to providing an “example” witness for the next Article 39(a) session to examine the viability of alternatives to closure for two reasons. First, an “example” witness would not assist the Court in testing whether alternatives short of closure are reasonable during portions of testimony from the remaining 27 witnesses. To the contrary, there are no alternatives that are reasonable because those portions of testimony for which closure is sought are entirely and inextricably linked to classified information.

I: PROVIDING AN “EXAMPLE” WITNESS TO TEST WHETHER ALTERNATIVES SHORT OF CLOSURE ARE VIABLE FOR ALL TWENTY-EIGHT WITNESSES IS UNPRECEDENTED AND WILL NOT ASSIST THE COURT IN DETERMINING WHETHER ANY SUCH ALTERNATIVES ARE REASONABLE UNDER RCM 806.

For closure inquiries, the Court must consider whether alternatives to closure exist and, if so, whether those alternatives are reasonable. See RCM 806(b)(2) (stating that courts-martial shall be open to the public unless, *inter alia*, “reasonable alternatives to closure were considered and found inadequate”). Generally, the determination of what portion of testimony is to be closed “must be made on a case-by-case, witness-by-witness, and circumstance-by-circumstance basis.” *ABC, Inc. v. Powell*, 47 M.J. 363, 365 (C.A.A.F. 1997). For closures relating to classified information, the Court in *Lonetree* is instructive. See *United States v. Lonetree*, 31 M.J. 849, 853 (N-M. C.M.R. 1990, *aff’d and rem’d*, 35 M.J. 396 (C.M.A. 1992).

In *Lonetree*, the appellant argued the military judge improperly closed the courtroom during classified portions of witness testimony by failing to make specific findings each time the court was closed and by failing to narrowly tailor each closure, thus denying the accused his right to a public trial under the Sixth Amendment. See *Lonetree*, 31 M.J. at 853. The Court disagreed. In determining whether specific findings are required, the Court delineated the distinction for cases involving closures to protect classified information. See *Lonetree*, 31 M.J. at 853 (stating that “Military Rule of Evidence 505 is directed towards the *information* sought to

be exempted from disclosure at a public trial”). The Court reasoned that when classified “information may be divulged by a number of witnesses or documents, or both, the focus of exclusion is upon that *specific information*” and the “specificity required [for closure] addresses the information to be protected.” *Lonetree*, 31 M.J. at 853 (emphasis added). On the other hand, for closures based on the rights of privacy of individuals, the Court noted that the focus is upon the individual rights requiring particularized rulings as to each individual situation. *Lonetree*, 31 M.J. at 853.

Under RCM 806(b)(2), the Court must consider whether alternatives to closure exist and, if so, whether those alternatives are reasonable. *See* RCM 806(b)(2). The defense proposes the Court adopt a trial-by-error approach to determine whether alternatives are reasonable, specifically that a witness be ordered to testify so that the parties may “attempt to elicit the same information through the use of alternatives.” The defense cites no authority supporting its proposal. Further, the United States is aware of no precedence involving a courtroom closure based on classified information where an “example” witness was ordered to testify for the *sole* purpose of testing whether alternatives are reasonable. Instead, military courts have relied largely upon classification determinations, the scope of testimony to be elicited in a closed session, and the Government’s rationale for requesting closure. *See e.g. Lonetree*, 31 M.J. at 853 (relying upon sworn affidavits identifying those witnesses who will testify about classified matters and the government’s rationale for requesting closure); *United States v. Anderson*, 68 M.J. 378 (C.A.A.F. 2010) (reviewing the evidence, classification declarations, and portion of testimony involving the classified information); Enclosures 1, 6, and 7 of Prosecution’s Supplement to Prosecution Response to Scheduling Order, dated 15 March 2013 (records from *United States v. Diaz*, 69 M.J. 127 (C.A.A.F. 2010) where the Court considered the invocation of the classified information privilege, a memorandum from the Original Classification Authority, a declaration that the document at issue was classified, and classification guides).

On 1 February 2013 and then with greater specificity on 15 March 2013, the United States delineated those portions of testimony relating to classified information that it seeks to elicit during a closed session, cited portions of the Original Classification Authority (OCA) classification guides confirming the information’s classification level, and stated its rationale for requesting closure. *See* AE 505. The United States has enclosed the applicable OCA classification guides, with pinpoint cites for the classified information that the United States requests to elicit in a closed session, to this filing. *See* Enclosures 1-2.¹ Enclosure 3 is a list of pinpoint citations to the applicable classification guides based on the most recent *Grunden* filing. Through these materials, the United States provided the Court with facts necessary to make specific findings for each individual closure, a standard beyond what is required under *Lonetree*.

The focus of closure should be upon that particular classified information set forth in Appellate Exhibit 505; put another way, the issue before this Court is whether alternatives short of closure exist for each piece of classified information and, if so, whether those alternatives for each piece of classified information are reasonable. Whether alternatives exist and are reasonable for the classified information that the United States intends to elicit from one witness is not indicative as to whether alternatives exist and are reasonable for classified information that

¹ Enclosure 1 is provided *ex parte* because the United States does not have approval to disclose this classified information to the defense.

the United States intends to elicit from another witness. That is true for all 28 witnesses, to include witnesses who share a “common” purpose. Whether alternatives exist and are reasonable for one OCA, subject matter expert or sentencing witness is not indicative as to whether alternatives exist and are reasonable for another OCA, subject matter expert, or sentencing witness. For example, the background, experiences, expertise, opinions, observations, and analyses of subject matter experts that may be elicited are completely different from one another and cannot be consolidated under one common legend of “code words.” The defense’s own filing under MRE 505(h) highlights its intent to explore these areas also during cross-examination. Therefore, should the Court require testimony through a mock-court session, to test whether alternatives are reasonable, it would be necessary for the Court to test the reasonableness of alternatives with each witness. Should the closure inquiry be focused at the information-level, as held in *Lonetree*, any such testimony would be of no value to the Court.

II: ALTERNATIVES SHORT OF CLOSURE ARE NOT REASONABLE FOR THIS SUBSET OF CLASSIFIED INFORMATION THAT IS INEXTRICABLY INTERTWINED AND REQUIRES CLOSURE TO PERMIT A CONTEXTUAL AND COMPLETE UNDERSTANDING OF THE CLASSIFIED TESTIMONY.

Military courts agree that reasonable alternatives should be employed to the extent possible, but not at the risk of causing utter confusion or impairing the ability to adequately present and explore the classified content, either by the parties, the Court, or the witness. *See Lonetree*, 31 M.J. at 854 (noting that although some unclassified information was disclosed in the closed session, “[f]urther bifurcation of other witnesses’ testimony, other than as occurred, was impracticable and would have created unnecessary chaos” and that “[t]he procedure utilized allowed both parties a reasonably normal context within which to pursue their respective positions”); Enclosures 1, 6, and 7 of the Prosecution’s Supplement to Prosecution Response to Scheduling Order, dated 15 March 2013 (records from *United States v. Diaz*, 69 M.J. 127 (C.A.A.F. 2010) where the Court ruled that court closure was “necessary to permit a contextual and complete understanding of the classified testimony”). In *Denver Post*, the Army Court of Criminal Appeals even noted that “in a few instances, the witnesses’ testimony could be fairly characterized as so inextricably linked to classified matters as to make it all properly received in a closed session.” *Denver Post Corp. v. United States*, 2005 WL 6519929, at 3 (A.C.C.A. 2005) (noting that this is an exception, not the rule).

The portion of testimony for which the United States requests closure is distinct from any other testimony the United States intends to elicit at trial. That testimony primarily consists of the following: (1) detailed factual observations necessary to put charged documents in their proper context with what was transpiring, both internationally and domestically; (2) factual observations of impact caused by the WikiLeaks disclosures not memorialized in writing; (3) expert opinions relating to the impact caused by the WikiLeaks disclosures not memorialized in writing; and (4) testimony relating to forensic analysis consisting of classified information so inextricably intertwined based on the alleged misconduct. The testimony for which closure is sought consists of numerous, inextricably commingled classified facts originating from several OCAs. This testimony cannot be sanitized merely by using a “code word” for a country, person, or name of a military operation. Instead, “code words” would also have to be employed, at a *minimum*, for past and current events taking place both domestically and internationally, the

reasons those events took place, the actions taken after those events took place, the reasons those actions were taken, the details of government operations, foreign persons, and so forth. In light of the defense specifically contesting whether the charged documents relate to the national defense, this type of detail can only be elicited in a closed session to permit a full contextual and complete understanding of the charged documents. For that limited portion of testimony, the alternatives to closure set forth in the prosecution's original *Grunden* filing cannot reasonably be employed without causing utter confusion to all parties involved, or impairing the ability to adequately present and explore the classified content, either by the parties, the Court, or the witness. See AE 479. To illustrate the inherent confusion with this specific type of testimony, the United States has enclosed the classified transcript of testimony provided during a closed session of the Article 32 investigation, along with an unclassified version of this testimony with the use of "code words" substituted over the original text to illustrate this point. See Enclosures 4 and 5 (the highlighted portions reflect the unclassified testimony directly related to the closed session within the classified portions of the enclosures). These enclosures also illustrate how a scalpel can be applied to such testimony and the topics can be discussed in open session and then more detail of those topics which are classified in closed session.

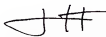
Practically, employing alternatives to this limited portion of testimony would frustrate justice, place an unreasonable burden upon the 28 witnesses and the Court Security Officer, and elevate the risk spillage of classified information. Based on the amount of, and inextricably commingling of, classified information through testimony for the information outlined with these witnesses, a legend of "code words" would be quite lengthy and, undoubtedly, would not be exhaustive. Until those witnesses are excused, the need for additional or modified "code words" for all parties to explore areas at trial is evitable. Further, should any witness seek to testify to matters outside the scope of this legend, immediate additions would be necessary.²

Further, no matter how detailed the legend may be, having these portions of testimony in open court would place an unreasonable burden on the 28 witnesses and the Court Security Officer. Requiring the Court Security Officer to monitor the proceeding with an incredibly lengthy and convoluted legend is impractical. Lastly, the risk of spillage is a *known* reality in this court-martial. Members of the public have already sought to reveal what has been redacted in Court filings and posted their conclusions on the Internet. See Enclosures 6-8 (Enclosure 6 is a printout of a website that was dedicated to determining what information was redacted during the Article 32. Enclosure 7 is the webpage if the user clicks on the highlighted text on page 17 of Enclosure 6. Enclosure 8 is the webpage if the user clicks on the highlighted text on page 18 of Enclosure 6). Overall, these enclosures show that a savvy spectator is able to piece together unclassified but protected information while conducting independent research. A sophisticated adversary of the United States would have greater resources and capabilities to perform this task, if given the opportunity, especially when it comes to classified information. Further, members of the public have brought recording devices to previous Article 39(a) sessions, which would allow a spillage to be recorded and distributed outside the control of the United States Government. See Enclosure 9. Based on these facts and the world-wide publicity of this case, should the Court not close the court for this testimony, the risk that foreign adversaries come into possession of classified information is a heightened possibility.

² The United States acknowledges that these issues exist for all witnesses relying on syllabi and legends.

CONCLUSION

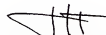
The United States respectfully objects to providing an "example" witness for the next Article 39(a) session to examine the viability of alternatives to closure for two reasons. First, an "example" witness would not assist the Court in testing whether alternatives short of courtroom closure during portions of testimony from the remaining twenty-seven witnesses are reasonable. To the contrary, reasonable alternatives are not available because those portions of testimony for which closure is sought are entirely and inextricably linked to classified information.


J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel

9 Encls

1. OCA Classification Guides [classified SECRET//NOFORN] [*ex parte*]
2. OCA Classification Guides [unclassified]
3. *Grunden* Motion with OCA Classification Guides Pinpoint Cites
4. Article 32 Transcript of SA David Shaver [classified SECRET//NOFORN]
5. Article 32 Transcript of SA David Shaver w/ Codeword Substitutions [classified SECRET//NOFORN]
6. Webpage Screenshot #1
7. Webpage Screenshot #2
8. Webpage Screenshot #3
9. Email from Mr. Coombs, 12 Mar 13

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel, via electronic mail on 3 April 2013.


J. HUNTER WHYTE
CPT, JA
Assistant Trial Counsel

Appellate Exhibit 512

Enclosure 1

105 pages

classified

"SECRET"

ordered sealed for Reason 2
and Reason 7 (government)

Military Judge's Seal Order

dated 20 August 2013

stored in the classified
supplement to the original
Record of Trial

UNCLASSIFIED

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)

PFC, U.S. Army,)

HHC, U.S. Army Garrison,)

Joint Base Myer-Henderson Hall)

Fort Myer, Virginia 22211)

Prosecution Objection to
Providing an "Example" Witness
to Examine the Viability of
Reasonable Alternatives to Closure

Enclosure 2

3 April 2013

UNCLASSIFIED

Encl 2 to
APPELLATE EXHIBIT 512
PAGE 1 OF 1
PAGE 1 OF 1 PAGES

FOR OFFICIAL USE ONLY

Headquarters
United States Central Command
MacDill Air Force Base, Florida 33621

Regulation
Number 380-14

UNITED STATES CENTRAL COMMAND SECURITY CLASSIFICATION GUIDE 0501

1. Purpose. This guide establishes the basic policies for proper classification, downgrading, and declassification of information related to the operations, facilities, communications, data collection and processing, warning, and other information pertaining to United States Central Command (USCENTCOM) and its components during normal periods and deployments for exercises and operations. This guide supercedes USCENTCOM Security Classification Guide 9901, dated 1 February 1999.
 2. Applicability. This guide applies to the Headquarters, USCENTCOM; its components; and those government agencies, civilian contractors, and personnel involved in the activities of USCENTCOM.
 3. Authority. The Original Classification Authority (OCA) for this guide is Lieutenant General Lance L. Smith, Deputy Commander, USCENTCOM. This classification guide reflects changes required by Executive Order (EO) 13292 dated 28 March 2003, "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information", and the Information Security Oversight Office (ISOO) Directive 1, 22 September 2003. Changes in classification markings are required in accordance with EO 12958, as amended. The classification authority for information covered under this guide shall be cited as shown below, along with the appropriate declassification instructions.
- DERIVED FROM: USCENTCOM Security Classification
Guide 0501, Dated: 1 January 2005
4. Effective Date. This guide is effective upon receipt.

*This is a new regulation

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

5. Conflict/Changes. If this security classification guidance imposes impractical controls, or if changes are deemed appropriate, the U.S. government activity or civilian contractor organization concerned should forward recommendations and supporting rationale to the USCENCOM SSO. Submission of such recommendations will not constitute authority to reclassify information and will not become an official change unless published as an update to this guide with the concurrence of the OPR.

6. Use and Reproduction of this Guide. This guide shall be used to determine the levels of the security classification to be assigned to information, systems, programs, plans, or projects associated with USCENCOM. It may be necessary to consult separate classification guides to determine the degrees of security classification with respect to individual systems/subsystems, programs, plans, or projects that are USCENCOM related. Reproduction of this guide is permissible.

7. Disclosure of Unclassified Information. DOD considers disclosure as the transfer of military information through approved channels to an authorized representative. When certain details of information are unclassified, it does not authorize automatic public disclosure. Proposed disclosure of unclassified information shall be processed through the Public Affairs Office (CCPA) and/or the Command Information Management Branch (CCJ6-PB), as appropriate. The term "disclosure" includes, but is not limited to, any technical data, articles, speeches, photographs, brochures, advertisements, presentations, and displays.

8. Disclosure of Classified Information.

a. To Other Government Agencies. Classified information regarding USCENCOM may be disclosed to other DOD components, Federal agencies, or U.S. industrial facilities, only to properly cleared persons on a need-to-know basis in accordance with DOD 5200.1-R and USCENCOM Regulation 380-1. It is the responsibility of the individual disclosing the information to verify the recipient's appropriate security clearance and need-to-know.

b. To Foreign Nationals. Classified information pertaining to USCENCOM-related matters will not be disclosed to foreign nationals, foreign governments, or international organizations

FOR OFFICIAL USE ONLY

without proper authorization per the National Disclosure Policy and USCENTCOM Regulation 380-5, upon coordination with CCJ2-FDO, the appropriate Director/Chief of Special Staff, and their designated Foreign Disclosure Representative.

c. Limitations. This guide should not be construed to allow the disclosure of proprietary information owned by private firms or citizens (i.e. patents, copyrights or trade secrets) to other contractors engaged in projects at USCENTCOM unless approved by the owner of such proprietary information.

9. Declassification and Downgrading. Information meeting the classification requirements of this guide shall remain classified as long as required by national security considerations. EO 12958, as amended provides uniform instructions for declassifying and downgrading national security information, including information relating to defense against transnational terrorism. These instructions are provided for each specific topic of information and they are not intended to be transcribed verbatim. They should be used to determine a specific date or event for declassification or downgrading. Specific declassification authority is not required to remark documents downgraded or declassified in accordance with instructions provided in this guide.

10. Organization of the Classification Guide (APPENDIX A).

a. Information Revealing. The "INFORMATION REVEALING" column states precisely the elements of information to be protected.

b. Classification. The "CLASS" column states which classification level applies to each element of information listed under the "INFORMATION REVEALING" column. The markings listed below are accompanied by descriptive extracts from DoD 5200.1-R:

(1) TOP SECRET. Applied to information, the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave damage* to the national security that the original classification authority is able to identify or describe.

(2) SECRET. Applied to information, the unauthorized disclosure of which reasonably could be expected to cause

FOR OFFICIAL USE ONLY

serious damage to the national security that the original classification authority is able to identify or describe.

(3) CONFIDENTIAL. Applied to information, the unauthorized disclosure of which reasonably could be expected to cause *damage* to the national security that the original classification authority is able to identify or describe.

(4) UNCLASSIFIED. Some UNCLASSIFIED information may be assigned FOR OFFICIAL USE ONLY (FOUO) status in the "REMARKS" column. FOUO is not a security classification, but a handling caveat. DOD 5400.7-R, DOD Freedom of Information Act Program, contains guidelines for properly marking, handling, and safeguarding FOUO information.

c. Declassification/Exemption. As of 22 September 2003, the use of X1, X2, X3, X4, X5, X6, X7, and X8 was no longer allowed as declassification markings. The "DECLASSIFY ON" column specifies the date or event for declassification or the 10-year automatic declassification exemption category as described in DOD 5200.1-R. If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority determines that the sensitivity of the information requires that it shall be marked for declassification for up to 25 years from the date of the original decision. When deciding how to complete the "Declassify on" line, an original classification authority will have the following choices:

- (1) A date or event less than 10 years.
- (2) A date 10 years from the date of the document.
- (3) A date up to 25 years from the date of the document.

d. Reason. The "REASON" column specifies the reason for classification, citing the appropriate category of information listed in Section 1.4 of EO 13292, as follows:

- (1) Military plans, weapons systems, or operations.
- (2) Foreign government information.

FOR OFFICIAL USE ONLY

(3) Intelligence activities (including special activities), intelligence sources or methods, or cryptology.

(4) Foreign relations or foreign activities of the United States, including confidential sources.

(5) Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism.

(6) United States government programs for safeguarding nuclear materials or facilities.

(7) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism.

(8) Weapons of mass destruction.

e. Remarks. The "REMARKS" column contains any other pertinent information for each element of information, as appropriate, to include downgrading instruction, FOUO designations, etc.

FOR OFFICIAL USE ONLY

11. PROPONENT. The proponent of this regulation is the Director of Intelligence, CCJ2. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQ USCENCOM, ATTN: CCJ2-SSO, 7115 South Boundary Boulevard, MacDill AFB, FL 33621-5101, (813) 827-6281/6282 Fax: (813) 827-5484 (DSN: 651).

FOR THE COMMANDER:



OFFICIAL:

JOHN G. CASTELLAW
Major General, USMC
Chief of Staff

ANITA H. WRIGHT
LCDR, USN
Chief, Business Management
Branch

DISTRIBUTION:

C (1 EA), G

FOR OFFICIAL USE ONLY

APPENDIX A
USCENTCOM Security Classification Guide 0501

MANPOWER, PERSONNEL, AND ADMINISTRATION (CCJ1)				
Information revealing	Classification	Declassification	Reason	Remarks
Country clearance requests	U	N/A	N/A	Will become classified if specific classified information is included (e.g., detailed travel itineraries of general/flag officers, etc.)
Daily personnel statistics	S	1 month	1.4(g)	Approximate numbers of deployed personnel may be released by the CCPA for official use

FOR OFFICIAL USE ONLY

INTELLIGENCE AND SECURITY (CCJ2/JICCENT)				
Information revealing	Classification	Declassification	Reason	Remarks
Information concerning CI/HUMINT and other sensitive intelligence sources and methods	S	10 years	1.4(c)	May be classified higher if it incorporates information of a higher classification or by direction of the CCJ2 OCA
Intelligence information obtained from CI/HUMINT	C	10 years	1.4(c)	If the source is not identified
Intelligence exchange agreements	S	10 years	1.4(b) / 1.4(c)	
Products of analysis by USCENTCOM intelligence analysts	S	10 years	1.4(c)	May be classified higher if it incorporates information of a higher classification or by direction of the CCJ2 OCA

FOR OFFICIAL USE ONLY

SECURITY (CCJ2-SSO)				
Information revealing	Classification	Declassification	Reason	Remarks
Approved modifications to the requirements of DOD 5200.1-R during operations	C	Upon completion of operation	1.4(g)	
Damage assessments conducted pursuant to the loss or compromise of classified information	C	10 years	1.4(g)	May be classified higher based on content
Exploitable information or personnel security weaknesses in OCONUS areas	C	Upon correction, elimination of weakness, or 10 years, whichever is sooner	1.4(g)	
General security countermeasures	U	N/A	N/A	
Loss of classified material	C	Upon regaining custody of material or following completion of damage assessment, whichever is later	1.4(g)	
Weaknesses in the application of security measures for safeguarding classified information during operations, in OCONUS locations, or during periods of increased threat	C	Upon correction of weakness or completion of the operation, whichever is sooner	1.4(g)	

FOR OFFICIAL USE ONLY

SYSTEMS (CCJ2-S)				
Information revealing	Classification	Declassification	Reason	Remarks
ALE password	TS	Upon change	1.4(a)	SCI
COLISEUM password	TS	Upon change	1.4(a)	SCI
DAWN/HOCNET password	S	Upon change	1.4(a)	
GALE password	TS	Upon change	1.4(a)	SCI
JWICS LAN/WAN user ID	U	N/A	N/A	
JWICS LAN/WAN password	TS	Upon change	1.4(a)	SCI
RMS password	TS	Upon change	1.4(a)	SCI
SAFE password	TS	Upon change	1.4(a)	SCI
Virus/network intrusions	S	Once neutralized	1.4(g)	
XDITDS password	TS	Upon change	1.4(a)	SCI

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

OPERATIONS (CCJ3)				
Information revealing	Classification	Declassification	Reason	Remarks
Exercises (CCJ3-E)				Separate classification guidance shall be issued by CCJ3-E for exercises. CCJ3-E will issue a by-country yearly guide or a guide for each specific exercise. For further information, contact CCJ3-E

FOR OFFICIAL USE ONLY

STRATEGIC DEPLOYMENT (CCJ3-S)				
Information revealing	Classification	Declassification	Reason	Remarks
C-Date/calendar date association	C	3 years after completion	1.4(a)	
Concept of operations	S	1 year after completion	1.4(a)	Confidential upon execution
Exercise name	U	N/A	N/A	
Exercise/operation location	S	Upon execution	1.4(a)	If classification/ declassification instructions are not specified by JCS/HN
Exercise/operation name associated with host nation (HN)	S	Upon execution	1.4(a) / 1.4(d)	If classification/ declassification instructions are not specified by JCS/HN
Exercise/operation name associated with participating units	S	Upon execution	1.4(a)	If classification/ declassification instructions are not specified by JCS/HN
Operation code words	S	1 year after completion	1.4(a)	Confidential upon execution
Participation of a specific individual in operation	U	N/A	N/A	
Participating units, including types, vulnerabilities, locations, quantities, readiness status, deployments, redeployments, and details of movement of U.S. and friendly forces in operation	S	Upon execution or following release by national command authorities, whichever is sooner	1.4(a)	If classification/ declassification instructions are not specified by JCS/HN
Information revealing	Classification	Declassification	Reason	Remarks
Units/HN association	S	1 year after completion	1.4(a) / 1.4(d)	Confidential upon execution

FOR OFFICIAL USE ONLY

LOGISTICS AND ENGINEERING (CCJ4/7)				
Information Revealing	Classification	Declassification	Reason	Remarks
Analysis and impact of all USCENTCOM AORs	C	Upon completion of mission	1.4(d) / 1.4(g)	Negotiations of construction projects, AIK, customs issues, etc
Bilateral OPLAN execution logistics and support requirements with AOR partners	C	10 years or upon completion of project, whichever is sooner	1.4(a) / 1.4(d)	
Characteristics of U.S. weapons and related sustainability	S	10 years	1.4(a)	May be classified higher upon direction of an OCA
Deployment/redeployment of units	C	Upon completion of mission or following release by national command authorities, whichever is sooner	1.4(a) / 1.4(g)	May be classified higher upon direction of the CCJ4/7 OCA
Force protection threat analysis	S	Upon completion of mission	1.4(g)	Includes intelligence efforts and threat weapons
Identification of forward headquarters	S	10 years	1.4(a) / 1.4(g)	Purpose of facility is classified. Description as school house" is unclassified.

FOR OFFICIAL USE ONLY

LOGISTICS AND ENGINEERING (CCJ4/7) Cont.				
Information Revealing	Classification	Declassification	Reason	Remarks
JAL fuel inventory	S	10 years or upon completion of mission, whichever is sooner	1.4(g)	Classified when inventory is related to days of war supply
MOBSTR-B	S	Upon completion of mission	1.4(g)	Location/capabilities of relay system for U2
Movement of ammunition, aircraft, personnel, units, or communications equipment	C	Upon completion of mission	1.4(a) / 1.4(g)	May be classified higher upon direction of an OCA
Movement of sensitive or critical supplies/personnel	C	Upon completion of mission	1.4(a) / 1.4(g)	May be classified higher upon direction of the CCJ4/7 OCA
Number of aircraft in AOR	S	Upon completion of mission	1.4(g)	Coalition aircraft report (If classification/declassification instructions are not specified by JCS/HN)
Proposed U.S. positions or strategy of negotiations	C	Upon completion of mission	1.4(a) / 1.4(d)	Negotiations of construction projects, assistance in kind (AIK), customs issues, etc.
War reserve stockage data	S	10 years	1.4(a) / 1.4(g)	

FOR OFFICIAL USE ONLY

PLANS AND POLICY (CCJ5)				
Information Revealing	Classification	Declassification	Reason	Remarks
Beddown sites	S	10 years or upon plan execution, if executed	1.4(a)	
Capabilities-based munitions requirements	S	10 years	1.4(a)	
Chemical/biological weapons and proliferation plans	S	10 years	1.4(a) / 1.4(h)	
Command and control relationships	U	N/A	N/A	
Commander's intent	S	10 years	1.4(a)	Confidential upon plan execution
Deception plans for operations	TS	10 years	1.4(a)	
Defended assets list (DAL)	S	10 years	1.4(a)	
Essential elements of friendly information (EEFI)	S	10 years	1.4(a)	Complete detailed list
Force lists	S	10 years	1.4(a)	Confidential upon plan execution
HN participation	S	10 years or upon plan execution, if executed	1.4(a) / 1.4(b)	
Joint monthly readiness review (JMRR)	S	10 years	1.4(a)	

FOR OFFICIAL USE ONLY

PLANS AND POLICY (CCJ5) Cont.				
Information Revealing	Classification	Declassification	Reason	Remarks
Location and designation of USCENTCOM representatives	U	N/A	N/A	
Mission statements	S	10 years	1.4(a)	Confidential upon plan execution
NBC operations	S	10 years	1.4(a)/1.4(h)	
Plan briefs	S	10 years	1.4(a)	
Plan phasing	S	10 years	1.4(a)	
Planning directives	S	10 years	1.4(a)	Confidential upon plan execution
Planning milestones, internal suspense dates	U	N/A	N/A	
Rules of engagement	S	10 years or upon plan execution, if executed	1.4(a)	
Strategic concepts	S	10 years	1.4(a)	
TPFDD plan identifiers, except:	U	N/A	1.4(a)	
- Aggregate tonnage/pax	U	N/A	N/A	
- U.S. unit name and destination com ined (except SOF)	U	N/A	N/A	
- U.S. unit name with EAD/LAD	U	N/A	N/A	
- U.S. unit name with UIC/ULN	U	N/A	N/A	

FOR OFFICIAL USE ONLY

PLANS AND POLICY (CCJ5) Cont.				
Information Revealing	Classification	Declassification	Reason	Remarks
- ULN and destination	U	N/A	N/A	
- ULN and EAD/LAD	U	N/A	N/A	
- Origin, UIC, and ULN	U	N/A	N/A	
- Flight plans for logistics support	U	N/A	N/A	
War plan short title combined with long title	S	10 years	1.4(a)	
War plan short title or long title standing alone	U	N/A	N/A	

FOR OFFICIAL USE ONLY

DELIBERATE WAR PLANS (CCJ5-P)				
Information revealing	Classification	Declassification	Reason	Remarks
Characteristics of U.S. weapons and related sustainability	S	10 years	1.4(a)	May be classified higher upon direction of an OCA
Communications effectiveness, sustainability, limitations	S	10 years	1.4(a)	
Concept of operations including order of battle, execution circumstances, operating locations, resources required, tactical maneuvers, deployments, actions and objectives	S	10 years	1.4(a)	Confidential upon plan execution
DEFCON meaning and status	S	10 years	1.4(a)	
Synchronization matrices	S	10 years	1.4(a)	
Plan(s) timelines	S	10 years	1.4(a)	
Flexible deterrent options	S	10 years	1.4(a)	
Estimates of operational effectiveness of intelligence, counterintelligence, rescue, and reconnaissance	S	10 years	1.4(a)	

FOR OFFICIAL USE ONLY

DELIBERATE WAR PLANS (CCJ5-P) Cont.				
Information revealing	Classification	Declassification	Reason	Remarks
Limitations and vulnerabilities of U.S. forces in the combat area	S	10 years	1.4(g)	
Location, itineraries, and travel modes of key U.S. and friendly military and civilian leaders	S	10 years	1.4(a)	Confidential upon execution of VIP travel
Nuclear weapons; potential use of	S	10 years	1.4(a) / 1.4(h)	
Operation code words	S	10 years	1.4(a)	
Participating units, including types, vulnerabilities, locations, quantities, readiness status, deployments, redeployments, and details of movement of U.S. friendly forces	S	10 years	1.4(a)	Confidential upon plan execution
Plan classification guide	C	10 years or upon plan execution, if executed	1.4(a)	
Planning assumptions	S	10 years or upon plan execution, if executed	1.4(a)	

FOR OFFICIAL USE ONLY

DELIBERATE WAR PLANS (CCJ5-P) Cont.				
Information revealing	Classification	Declassification	Reason	Remarks
Status and details of U.S. alliances, including status of forces, deployment rights, privileges, airfield use, and port availability	S	10 years	1.4(a) / 1.4(d)	
Friendly centers of gravity	S	10 years	1.4(a)	
War termination objectives	S	10 years	1.4(a)	
End state of plan	S	10 years	1.4(a)	
Target area weather information	S	10 years or upon plan execution, if executed	1.4(a)	
Top secret options; discussion of	TS	10 years	1.4(a)	
Limitations and vulnerabilities of U.S.	S	10 years	1.4(g)	

FOR OFFICIAL USE ONLY

COMMAND AND CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS (CCJ6)				
Information revealing	Classification	Declassification	Reason	Remarks
Communications networks, users, frequencies, call signs, HJ times, and identification of net control stations	S	When superceded	1.4(a) / 1.4(g)	
COMSEC incidents/violations	C	10 years	1.4(g)	
Composite list of COMSEC short titles	C	10 years	1.4(c)	
Cryptology	S	10 years	1.4(c)	
Communication outages that degrade command and control capability	S	Upon restoration of capability	1.4(g)	
Scheduled down times of communications systems	S	10 years	1.4(g)	
GCCS User ID	U	N/A	N/A	
GCCS Password	S	When changed	1.4(a)	
Specific locations of deployed communications units	S	Upon redeployment	1.4(a) / 1.4(g)	
Specific locations or countries planned for employment of elements of Defense Communications Systems - Central Area (DCS-CA)	S	10 years	1.4(d)	

FOR OFFICIAL USE ONLY

COMMAND AND CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS (CCJ6) Cont.				
Information revealing	Classification	Declassification	Reason	Remarks
Specific locations or countries in which DCS-CA are employed	S	10 years	1.4 (d)	
Details revealing specific units supported by DCS-CA	S	10 years	1.4 (c) / 1.4 (g)	
Details revealing force locations, by type, for war plan employment of DCS-CA	S	10 years	1.4 (a)	
Specific locations or countries in the AOR in which communication equipment is identified as supporting the DCS-CA	S	10 years	1.4 (d)	
Identification of an operational shortfall or limitation in war-fighting capabilities of DCS-CA	S	Upon correction	1.4 (g)	
Details of the capability required to achieve the initial operational capability of DCS-CA	S	Upon full operational capability	1.4 (g)	

FOR OFFICIAL USE ONLY

COMMAND AND CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS (CCJ6) Cont.				
Information revealing	Classification	Declassification	Reason	Remarks
A description of the DCS-CA system and details of the capability required to achieve full operational capability	U	N/A	N/A	
A description of the composition of a DCS-CA node at full operational capability	U	N/A	N/A	
Characteristics of the DCS-CA	U	N/A	N/A	
Cost/Budget data on the DCS-CA	U	N/A	N/A	
Identification of the agencies responsible for the various aspects of system acquisition, implementation, operation, and maintenance	U	N/A	N/A	
Required capability dates, initial operational capability, and full operational capability dates	U	N/A	N/A	
Frequencies lists	U	N/A	N/A	
Contingency and Operational Joint Communications Electronics Operating Instructions (JCEOI)	S	When superceded	1.4(a)	Unclassified for training within the U.S. Releasable to MNF when part of Coalition

FOR OFFICIAL USE ONLY

COMMAND AND CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS (CCJ6) Cont.				
Information revealing	Classification	Declassification	Reason	Remarks
Frequency lists used in the AOR associated with the location/coordinates, date/times of use, operating units, and detailed purpose of the frequency (Example: Force Protection Net)	S	When superseded	1.4(a)	List of frequencies alone are Unclassified
Frequency lists used in the AOR required for coordination with the host nation may only be associated with the location/coordinates, date/times of use of the frequency (Example: Land Mobile Radio Communications)	U	N/A	N/A	Information required to be released is considered FOUO (DOD 5400.7-R)
Joint Restricted Frequency Listings (JRFL)	S	When superceded	1.4(a) / 1.4(c)	Releasable to MNF when part of the Coalition. Determined by Command Electronic Warfare Officer (EWO)

FOR OFFICIAL USE ONLY

RESOURCES AND ASSESSEMENT (CCJ8-AR)				
Information revealing	Classification	Declassification	Reason	Remarks
Products of analysis by USCENCOM operations research analysts	S	10 years	1.4(a)	May be classified higher if it incorporates information of a higher classification or upon direction of an OCA
Requirements documents identifying USCENCOM future operational needs in support of CDR USCENCOM strategy	S	10 years	1.4(a) / 1.4 (b) / 1.4 (e) / 1.4 (g)	

FOR OFFICIAL USE ONLY

SCIENTIFIC ADVISOR (CCJ8-TI)				
Information revealing	Classification	Declassification	Reason	Remarks
Vulnerabilities of new military technologies	S	10 years or upon correction, if corrected	1.4(e) / 1.4(g)	
New operational concepts based on application of new technologies	S	25 years	1.4(e)	
Requirements documents identifying critical military deficiencies	S	10 years	1.4(g)	

FOR OFFICIAL USE ONLY

COMMAND GROUP (CCCC)				
Information revealing	Classification	Declassification	Reason	Remarks
Detailed travel itinerary of USCENTCOM Commander	S	Upon completion of travel	1.4(a) / 1.4(g)	Classified when information reveals name/title associated with dates/times or locations
Detailed travel itineraries of General/Flag officers and civilian equivalent	C	Upon completion of travel	1.4(a) / 1.4(g)	Classified when information reveals name/title associated with dates/times or locations

FOR OFFICIAL USE ONLY



Attack the Network – Defeat the Device – Train the Force

SECURITY CLASSIFICATION GUIDE

for

JOINT IMPROVISED EXPLOSIVE DEVICE DEFEAT ORGANIZATION (JIEDDO)

DISTRIBUTION STATEMENT D: Distribution authorized to the Department of Defense and U.S. DoD contractors only, administrative or operational use, effective the approval date of this document. Other requests for this document shall be referred to the JIEDDO Security Office.

This document contains information
EXEMPT FROM MANDATORY DISCLOSURE
Under the Freedom Of Information Act (FOIA).
Exemption 2 applies.

1

FOR OFFICIAL USE ONLY

APPELLATE EXHIBIT 512, ENCL 2
PAGE REFERENCED:
PAGE OF PAGES

FOR OFFICIAL USE ONLY

Security Classification Guide

for

Joint Improvised Explosive Device Defeat Organization (JIEDDO)

Date: _____

Approved By: _____
Michael D. Barbero, LTG
Director
Joint IED Defeat Organization

Issued By: Joint IED Defeat Organization
5000 Army Pentagon
Washington, DC 20310-5000

Action Officer: Mr. John E. Nimitz
Security Officer/SSR
Joint IED Defeat Organization
703-601-4744

FOR OFFICIAL USE ONLY

1. PURPOSE

This Security Classification Guide (SCG) is a living document that provides guidance and instructions on the classification, marking and distribution of information involved in the development and eventual employment of tactics, techniques, procedures (TTP) and technologies that enable the Joint Improvised Explosive Device Defeat (IED) Organization (JIEDDO) to defeat the IED threat. This SCG addresses security measures to safeguard developmental efforts within the organization as well as already developed end items that require ongoing protection measures. As the organization matures, JIEDDO will update the SCG to address additional IED defeat developmental efforts requiring protection. Future revisions to this SCG will update declassification dates in light of fielding dates and other program milestones, as well as technology commercialization and/or obsolescence. Any suggested changes or updates to this SCG will be provided in writing to the Office of Primary Responsibility (OPR) as indicated in paragraph three.

2. AUTHORITY

This SCG is issued under authority of Executive Order (E.O.) 12958, as amended 25 March 2003, and DoDI 5200.1-R (Information Security Program). This SCG constitutes authority and may be cited as the basis for classification, downgrading, or declassification of material related to the JIEDDO activities in support of DoD Directive 2000.19E, Joint Improvised Explosive Device Defeat. Unless otherwise noted, information or material identified as CLASSIFIED by this SCG is classified by authority of the JIEDDO Original Classification Authority identified on the title page.

3. OFFICE OF PRIMARY RESPONSIBILITY (OPR)

This SCG is issued by and all inquiries for information concerning its content should be addressed to the Joint Improvised Explosive Device Defeat Organization (JIEDDO), Attn: Director, 5000 Army Pentagon, Washington DC 20310-5000.

4. CLASSIFICATION CHALLENGES

Questions concerning the content and interpretation of this SCG should be directed to the issuing activity. If the security classification imposed by this SCG is considered impractical, documented and justified recommendations should be made through appropriate channels to the issuing activity. If current conditions, progress made in this effort, scientific or technological developments, advances in the state-of-the-art or other factors indicate a need for changes, similar recommendations should be made. Pending a final decision, the information involved will be protected at either the currently specified level or the recommended level, whichever is higher. All users of this SCG are encouraged to assist in improving its currency and adequacy. Any classification challenges should be brought to the attention of the OPR.

FOR OFFICIAL USE ONLY

5. REPRODUCTION, EXTRACTION AND DISSEMINATION

Copies of this SCG and all extracts thereof will be made, stored, and transmitted in accordance with (IAW) authorized procedures corresponding to the classification of the information involved. Authorized recipients of this SCG may reproduce, extract, and disseminate the contents of this SCG, as necessary, for use by specified groups, including industrial activities that are involved in IED Defeat development, test, or operations.

6. PUBLIC RELEASE

The fact that this SCG contains certain details of unclassified information does not permit automatic public release of the information. Proposed public disclosures of the JIEDDO's unclassified information regarding the technologies and activities shall be processed through appropriate channels for approval to publish. Requests for public release certification must be submitted in accordance with DoD Directive 5230.9 (Clearance of DoD Information for Public Release), DoD Regulation 5400.7 (DoD Freedom of Information Act Program), and the Industrial Security Manual for Safeguarding Classified Information (Section 5 Disclosure). Defense contractors, military members as well as government service employees shall comply with DoD Manual 5220.22-M (National Industrial Security Program Operational Manual (NISPOM)) and other requirements that may be directed by the Government.

Only information that has been reviewed and certified for public release may be released. However, the decision or authority to release information belongs to the Public Affairs office. The OPR will process requests for approval as outlined below.

Any proposed release to the public of official information pertaining to the JIEDDO must be forwarded to the JIEDDO, STRATCOM for review and further processing. The term "release" applies, but is not limited to, articles, speeches, briefs, papers, photographs, brochures, advertisements, displays, presentations, etc., on any JIEDDO related activity. It is incumbent upon defense contractors, or other agencies, to screen all information submitted by them for the material certification to ensure that it is both unclassified and technically accurate. Letters of transmittal shall contain certification to this effect. The number of copies produced, and distribution of the document, must be strictly controlled until review is completed. If suspected classified information is found during the review process, all holders of the document will be informed of the degree of protection required. When doubt exists concerning the classified status of a proposed release pertaining to the JIEDDO, Security will render the final decision. The material submitted for review must include a valid suspense date, if applicable. Requests for public release certification, according to DoD Manual 5220.22-M, NISPOM (attachment to DD Form 441, Security Agreement), must be submitted to the JIEDDO, STRATCOM for review and further processing. Electronic copies (unless submitted via Secret Internet Protocol Router Network (SIPRNet)) of the proposed public release material must be submitted to JIEDDO, STRATCOM at least two weeks before approval is needed.

FOR OFFICIAL USE ONLY

Approval for public release does not necessarily satisfy export-licensing requirements of the Departments of State and Commerce. Export-controlled material will not be entered into the security review channels for public release approval to circumvent the licensing requirements of the Departments of State and Commerce.

Release of Program Data on the World Wide Web: Extreme care must be taken when considering information for release onto publicly accessible or unprotected World Wide Web sites. In addition to satisfying all of the aforementioned approval provisions, owners and/or releasers of information proposed for such release must ensure that it is not susceptible to compilation with other information to render sensitive or even classified data in the aggregate. The search and data mining capabilities of Web technology must be assessed from a risk management perspective. If there are any doubts, do not release the information!

Release of information to foreign government service employees, international organizations and/or their representatives: Any military activity or defense contractor receiving a request for, or proposing to release information on this program will forward such requests/proposals to the OPR, after compliance with the following:

- Military activities will comply with the National Policy and Procedure for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1).
- Defense contractors will comply with the Department of State International Traffic in Arms Regulation (ITAR).

NOTE: Foreign national employees of the contractor or sub-contractor, including those possessing reciprocal clearances, are not authorized access to classified information resulting from or used in the performance of their contract unless authorized in writing by the OPR. Contractors shall ensure that this SCG, including all applicable standard security precautions and regulations identified in their DD Form 254, Contract Security Requirement, are complied with. Prime contractors are responsible for ensuring each of their subcontractors are aware of, and comply with, these requirements. Material proposed for release by subcontractors will be routed through their prime contractor.

Release of information to the United States Agencies: Requests will be submitted to the OPR.

Release of information at symposia, seminars, and conferences: Requests for such releases of classified information shall be submitted to the OPR for review and approval. Material will be submitted a minimum of six weeks prior to proposed release date in electronic format. Any information authorized for release will reflect that the work reported upon is sponsored by the DoD. If foreign nationals are expected to be present at such a conference, the provisions of paragraph 7 below must be followed.

FOR OFFICIAL USE ONLY

Use of information or data classified by a foreign government: If information or data has been previously classified by a foreign government, this information or data will be classified at a level which will accord at least the same degree of protection as provided by the foreign government classification. This procedure will be adhered to even though a higher classification than that normally imposed by the U.S. for the same type of information will result.

7. FOREIGN DISCLOSURE

Foreign disclosure is the sharing of US classified information with foreign governments or international organizations in support of established or approved planned international programs. Any disclosure to foreign officials of information classified by this SCG shall be in accordance with the procedures set forth in DoD Directive (DoDD) 5230.11, DoDI 5230.27 and National Disclosure Policy (NDP-1). A foreign disclosure review shall be conducted prior to issuance of any solicitation. This review should result in a determination regarding which foreign governments and international organizations (and their industrial entities) will be permitted to participate in the solicitation.

General Release Guidance: Classified information is only released to properly cleared persons on a need-to-know basis and through government-to-government channels. It is the responsibility of the individual actually releasing the information to verify that the recipient is a foreign official authorized to receive classified information on behalf of his/her government or international organization and that information has been properly approved for release. JIEDDO personnel originating material classified by this guide will mark it as it is created in accordance with DoDI 5200.1-R, "Information Security Program," January 1997. JIEDDO information developed within combined spaces is presumed to be releasable to foreign nations represented in those spaces and should be marked "[CLASSIFICATION]/REL TO USA, [COUNTRY OR ORGANIZATION CODE]." When information is derived from multiple sources, the most restrictive handling and declassification instructions apply to the derived document. Classified information not explicitly marked releasable to a particular country shall not be released without proper authorization from the originating Foreign Disclosure Officer.

According to DoDD 5230.11, under conditions of actual or imminent hostilities such as Operation Iraqi Freedom or Operation Enduring Freedom, any unified or specified commander may disclose classified military information (CMI) through TOP SECRET to an actively participating allied force when support of combined combat operations requires the disclosure of that information. Under such circumstances, the Chairman, National Disclosure Policy Committee will issue further guidance determining any limitations that should be imposed on continuing disclosure of that information. When an authorized disclosure official (such as a Foreign Disclosure Officer (FDO)) has made a determination that CMI originated by JIEDDO is releasable under these conditions, the FDO should mark that information "[CLASSIFICATION]/REL TO USA, [COUNTRY OR ORGANIZATION CODE]," and forward an information copy to the JIEDDO FDO. A foreign disclosure review shall be conducted prior to issuance of any solicitation. This review should result in a determination regarding their foreign governments and

FOR OFFICIAL USE ONLY

international organizations (and their industrial entities) permitted to participate in the solicitation.

8. FOREIGN GOVERNMENT INFORMATION AND FOREIGN MILITARY SALES

U.S. government information is furnished upon the condition that it will not be released to other nations without specific authority of the DoD of the United States. Subject release of information provides that individual or corporate rights originating the information will be provided substantially the same degree of security afforded it by the Department of Defense of the United States.

9. FOR OFFICIAL USE ONLY (FOUO) CAVEAT

For Official Use Only (FOUO) is not a security classification. FOUO information has not been given a security classification pursuant to the criteria in this SCG, but may be withheld from the public for one or more of the reasons cited in EO 12958, as amended, and DoDI 5200.1-R. Information so designated in this SCG that warrants FOUO markings will be handled and protected in accordance with regulations. The SCG for Freedom Of Information Act (FOIA) markings is intended solely as a guide. One, none or all of the suggested FOIA exemptions may apply to particular information depending on the particular facts of the information being protected or disclosed.

**This document contains information EXEMPT
FROM MANDATORY DISCLOSURE under the
FOIA. Exemption(s) . . . apply/applies.**

**ALL Freedom of Information Act (FOIA) exemptions Identified in this
SCG:**

Number 1. Material appropriately classified by this SCG is similarly exempt from disclosure as National Security Information under FOIA.

Number 2. Related solely to the internal personnel rules and practices of the DoD or any of its components. Records containing or constituting statutes, rules, regulations, orders, manuals, directives, instructions, and security classification guides. This classification encompasses "High 2" information (i.e., information that would allow persons to circumvent or undermine JIEDDO's internal practices) and "Low 2" information (i.e., information of a trivial administrative nature.)

Number 3. Records protected by another law that specifically exempts the information from public release. Applicable to technical Controlled Unclassified Information (CUI).

Number 4. Containing trade secrets or commercial or financial information that a DoD Component receives from a person or organization outside the Government which is likely to cause substantial harm to the competitive position of the source, impair the Government's ability to obtain necessary information in the future, or impair some other

FOR OFFICIAL USE ONLY

legitimate Government interest. Some examples: Commercial or financial information received in confidence in connection with bids, contracts, or proposals; statistical data and commercial or financial information concerning contract performance, income, etc.; personal statements given in the course of inspections, investigations, or audits; financial data provided in confidence by private employers in connection with locality wage surveys; scientific and manufacturing processes or developments concerning technical or scientific data or other information submitted with an application for a grant or with a report while research is in progress; technical or scientific data developed by a contractor or subcontractor exclusively at private expense and technical or scientific data developed in part with federal funds and in part at private expense; computer software which is copyrighted; or, proprietary information submitted strictly on a voluntary basis.

Number 5. Subjective evaluations that are reflected in records pertaining to the decision-making process of an agency. Examples are: advice, suggestions or evaluations prepared on behalf of the DoD; non-factual portions of evaluations by DoD component personnel of contractors and their products; information of a speculative, tentative or evaluative nature; trade secret or other confidential research development; and portions of official reports on inspection, reports of the IG, audits, investigations, or surveys pertaining to safety, security, or the internal management, administration or operation of one or more DoD components.

10. DISTRIBUTION STATEMENT

Distribution statements are required to be placed on all technical documents no matter if they are classified or unclassified. Export controlled warning notices will be applied only to technical documents containing critical technology. These notices will be placed on the front cover or first page of the document. When possible, parts that contain information creating the requirement for a distribution statement or other warning notice shall be prepared as an appendix to permit broader distribution of the basic document.

Technical documents contain information (experimental, developmental, engineering works) that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul material. The information may be in text, graphic, or pictorial form.

The following statements will be applied to all technical documents as defined as above:

<p>DISTRIBUTION STATEMENT D: Distribution authorized to the Department of Defense and U.S. DoD contractors (fill in reason) (date of determination). Other requests for this document shall be referred to the JIEDDO Security Office.</p>

Reasons for applying distribution D:

FOR OFFICIAL USE ONLY

Foreign Government Information: To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information.

Administrative or Operational Use: To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.

Software Documentation: Releasable only in accordance with DoD Instruction 7930.2, Automatic Data Processing (ADP) software exchange and release.

Transfer of data from SIPR to a CD: Transfer of data from SIPR to a CD: Any data that needs to be transferred from SIPR to a CD must be done in accordance with US CYPERCOM CTO 10-133. Currently J6 and STRATCOM are the only authorized divisions that transfer data. All CD with SIPR Data or higher must bear the proper security marks (AR 380-5). Any CD(s) that needs to be mailed/hand carried out of the Polk building must go through JIEDDO Security. For further guidance, please contact JIEDDO Security.

Critical Technology: To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of DoDD 5230.25. Apply the following notice to the front cover or title page:

Warning – This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, USC, Sec 2751 etc) or the Export Administration Act of 1979, as amended (Title 50, USC, App 2401 etc). Violations of these export laws are subject to severe criminal penalties.

Specific Authority: To protect information not specifically included in the above reasons and discussions, but which requires protection in accordance with valid documented authority such as executive orders, classification guides, DoD or DoD component regulatory documents. When filing in the reasons, cite "Specific Authority (identification of valid documented authority)."

At times, the application of a different distribution statement may be necessary to facilitate sharing between U.S. government agencies (Distribution Statements B and C) or to limit dissemination based upon the Director's discretion (Distribution Statement F). Further exceptions for the use of another distribution statement shall be submitted to the JIEDDO Security Office, in writing, with justification.

FOR OFFICIAL USE ONLY

11. DISCLOSURE OF INTELLIGENCE/THREAT INFORMATION

Data or information relating to threat systems or other intelligence derived material must bear the security markings of that intelligence/threat material. All dissemination of intelligence / threat information is controlled by the Director, COIC. Intelligence/threat information may be reproduced, released to subcontractors, provided instructions, and procedures approved by the COIC Director. Intelligence/threat information may be reproduced, released to subcontractors, provided instructions, and procedures approved by the Senior Intelligence Officer (SIO) are followed. Questions regarding such releases shall be referred to the SIO.

12. LOSS, COMPROMISE, OR SUSPECTED COMPROMISE

Report the loss, compromise, or suspected compromise of classified JIEDDO information or material to the JIEDDO Security Office, 703-601-4744, within 24 hours of the incident.

13. COMPILATION OF INFORMATION.

In some circumstances, classification may be required if the compilation of unclassified items of information provide an inference that warrants classification. Similarly, a higher classification may be assigned to a compilation of information if the compilation provides an added factor that warrants higher classification than that of its component parts. Classification on this basis will be used sparingly, and complete justification of this classification method will be stated on the title or first page of the document. The classification and marking process is as follows:

- When a document comprises individually unclassified items of information is classified, by compilation, the overall classification shall be marked conspicuously at the top and bottom of each page and the outside front and back covers (if applicable). An explanation of the basis for classification by compilation shall be placed on the face of the document or included in the text.
- If portions, standing alone, are unclassified, but the document is classified by compilation or association, those portions shall be marked "U" and the document and pages shall be marked with the classification of the compilation. An explanation of the classification or the circumstances involved with association must be included.
- If individual portions are classified at one level and the compilation is a higher classification, each portion shall be marked with its own classification and the document and pages shall be marked with the classification of the compilation. An explanation of the classification by compilation is required.

FOR OFFICIAL USE ONLY

14. REASONS FOR CLASSIFYING

The reasons for classifying information in this SCG are in accordance with Part I, Section 1.4, Executive Order 12958 (as amended). They are:

- 1.4a – Military plans, weapons systems, or operations
- 1.4b – Foreign government information
- 1.4d – Foreign relations or foreign activities of the United States, including confidential sources; scientific, technological, or economic matters relating to national security
- 1.4 e – Scientific, technological, or economic matters
- 1.4 g – Vulnerabilities or capabilities of the system, installation, projects, or plans relating to the national security

15. DEFINITIONS

Classified Performance Capabilities or Limitations: Information that if disclosed would;

- 1) damage national security through facilitating adversary denial, degradation, disruption, deception, or destruction of mission essential or critical system(s), or
- 2) would require major modifications to an acquisition program or operational system to maintain the technological advantage of the system during its projected operational life time.

Compromise a Future Capability: Anything not in the inventory now and is planned to be developed; not a current capability. Applies to research, development and acquisition efforts.

Confidential: Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to national security that the original classification authority is able to identify or describe.

Critical Information: TBD by the supported organization. Different organizations may deem information differently as to its criticality. Determination and defense of information as critical is up to the supported organization.

Critical Program Information (CPI): Information, technologies, or systems that, unto themselves, if compromised would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction.

Effectiveness of Forces: TBD by supported organization. Usually refers to squad to division level. Different organizations may deem information differently as to its impact on the effectiveness of forces. For example; information that may impact the effectiveness of a Special Forces unit compared to a Battalion is potentially considerable. Determination and defense of information is up to the supported organization.

FOR OFFICIAL USE ONLY

Effectiveness of Major Forces: TBD by supported organization. Usually refers to theater level; unified command; combination of Military Departments (MILDEPS). Different organizations may deem information differently as to its impact on the effectiveness of major forces. Determination and defense of information is up to the supported organization.

Enhanced System Capability: An improvement over existing performance or capabilities found on similar systems.

Low- Level Intelligence Collection Capability: Focused on low- level counterintelligence, Human Intelligence (HUMINT) sources, e.g., bartender, "beat cop," or low- level detection capability, e.g., unattended ground sensors.

Mission Critical: A mission essential item whose disruption or destruction immediately degrades the ability of the force to command, control, or effectively conduct combat operations. For example, disruption or destruction of the mechanism used to fuse a system-of-systems (e.g., C4ISR) would result in the immediate inability for the separate system to act in concert as a system-of-systems.

Mission Essential: Those items required to support approved emergency and/or war plans, and where those items are used to:

- 1) destroy the enemy or the enemy's capacity to continue war;
- 2) provide battlefield protection of personnel;
- 3) communicate under war conditions;
- 4) detect, locate, or maintain surveillance over the enemy;
- 5) provide combat transportation and support of men and materiel; and/or
- 6) support training functions.

National Military Objectives: Protect the United States against external attacks and aggression; prevent conflict and surprise attack, and prevail against adversaries. These are the ends of the strategy and help to assure allies and friends, dissuade adversaries, and deter aggression and coercion while ensuring the armed forces remain ready to defeat adversaries should deterrence and dissuasion fail. They serve as benchmarks to assess levels of risk and help to define the types and amounts of military capabilities required.

National Objectives (for DoD): The aims derived from national goals and interests, toward which a national policy or strategy is directed and efforts and resources of the nation are applied.

National Security Strategy (for DoD): The art and science of developing, applying, and coordinating the instruments of national power (diplomatic, economic, military, and informational) to achieve objectives that contribute to national security. Also called national strategy or grand strategy.

FOR OFFICIAL USE ONLY

NOFORN: (NOT RELEASABLE TO FOREIGN NATIONALS) Under authority of Director of Central Intelligence, this marking is used for identified *classified intelligence* that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-US citizens without permission of the originator and in accordance with provisions of DCID 6/7 and NDP-1. Cannot be used with REL TO [country codes] or EYES ONLY on page markings (when a document contains both NOFORN and REL TO or NOFORN and EYES ONLY portions, NOFORN takes precedence for the markings at the top and bottom of the page).

Reveal a National Security Objective: Fact of statement that would reveal an undisclosed objective or intention—that is covert in nature. Details of how we plan to achieve national security objectives (primarily planning oriented).

Secret: Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Senior Leadership: President of the US (POTUS); Cabinet Members, Pentagon Senior Leadership, etc.

Sensitive Information: TBD by the supported organization. Different organizations may deem information differently as to its sensitivity. Determination and defense of information as sensitive is up to the supported organization.

Sensitive Intelligence Collection Capability: To be determined by the user or developer of that capability.

Significant Impairment: Any characteristic or concept, design or component that offers a technical disadvantage of enough magnitude to be potentially disruptive in an operational or advanced system.

State of the Art: The highest level of development, as of a device, technique, or scientific field, achieved at a particular time. For a system or technology that has no known baseline to determine its relative level of development, the very nature of it being the first of a kind, makes it state of the art.

Strategic Advantage: Operational superiority provided via military instruments that enables one nation or group of nations effectively to control the course of a military or political situation beyond a battle or engagement.

Strategic Disadvantage: Inverse of strategic advantage (see above definition).

FOR OFFICIAL USE ONLY

Tactical Advantage: Operational superiority provided via unit and system performance and capabilities during battles and engagements planned and executed to accomplish military objectives assigned to tactical units or task forces.

Tactical Disadvantage: Inverse of tactical advantage (see above definition).

Threaten the Country's Ability to Wage War: Identification of details of war plans that would reveal overall objectives or intentions.

Top Secret: Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security that the original classification authority is able to identify or describe.

Weaken the Country's Ability to Wage War: Identification of specific details of war plans in a theater of operation including use of tactical capabilities and mission essential items.

Significantly Weaken the Country's Ability to Wage War: Identification of specific dependencies and objectives in a theater of operation or sub area of a Unified Command to include strategic capabilities and mission critical items.

Threaten the International Position of the US: Damage US credibility with a foreign government.

Weaken the International Position of the US: Negative impact to the international position of the US and its ability to negotiate with foreign governments.

Significantly Weaken the International Position of the US: Inability of the US to successfully negotiate with a foreign government for a significant period of time.

Unique and Fragile Intelligence Collection Capability: To be determined by the user or developer of that capability.

FOR OFFICIAL USE ONLY

Only trained FDOs who have been issued a Delegation of Disclosure Authority Letter (DDL) can authorize the disclosure or release of classified military information to authorized representatives of foreign governments or international organizations as outlined in this guide.

ADMINISTRATION DATA

Element	Level	Duration	Remarks
JIEDDO Goal, Mission and Purpose			
JIEDDO mission	U		Public Release and Distribution Statement A applies for the following description: JIEDDO shall focus (lead, advocate, coordinate) all Department of Defense actions in support of Combatant Commanders and their respective Joint Task Forces' efforts to defeat improvised explosive devices as weapons of strategic influence. (DoDD 2000.1E)
JIEDDO organizational structure (Line and block chart identifying position only)	U		
JIEDDO organizational structure (Line and block chart identifying personnel by name)	U		Mark and handle as FOUO, FOIA exemption 2 applies.
JIEDDO Goals and Objectives	U		Mark and handle as FOUO, FOIA exemption 2 applies. Specific technological goals and objectives associated with real or postulated threats will be addressed by other portions of this SCG
JIEDDO Resources			
Financial plans	U		
Financial plans with classified program Names	U		Classify as directed by program security classification guide, FOIA 1(b)(2)(a).
JIEDDO budget	U		
Cost, pricing, or funding for individual systems, subsystems, or components	See Remarks		If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies. FOIA exemption 4 may apply to certain proprietary or trade secret information provided by vendors.

FOR OFFICIAL USE ONLY

			If individual project budget reveals a sensitive relationship between the JIEDDO and other DoD organizations, US government organizations, or a foreign government or foreign owned company then classify in accordance with the guidance provided by the other organization, government, or the contractor relationship portion of this document.
Budget levels for projects	See Remarks		If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies. If individual project budget reveals a sensitive relationship between the JIEDDO and other DoD organizations, US government organizations, or a foreign government or foreign owned company then classify in accordance with the guidance provided by the other organization, government, or the contractor relationship portion of this document..
Production quantities and delivery rates	U		If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies.
Manpower, overall by year, category, skill, and system	U		
Manpower, overall by year, category, skill, system, and individual name	U	If classified, declass in accordance with proponent SCG.	Mark and handle as FOUO, FOIA exemption 2 applies.
Identification of a particular installation, facility or range associated with the JIEDDO	U-S		Classify as directed by program security classification guide.
Aggregate number of C-IED systems deployed in a particular theater of operation or to a particular unit	See Remarks		Peacetime Situations: Derivative according to documents such as Table or Organization and Equipment. Combat Situations: Derivative according to operational SCG such as MNF-I or OEF SCG.
JIEDDO Schedules			
Organization master schedule	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Specific program/project status	U-S		Mark and handle as FOUO, FOIA exemption 2 applies.
Development milestones	U-S		Mark and handle as FOUO, FOIA exemption 2 applies.

FOR OFFICIAL USE ONLY

Procurement milestones	U-S		Mark and handle as FOUO, FOIA exemption 2 applies.
Contractor Relations			
Partial or full list of contractors producing or procuring IED defeat systems or component pieces	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Data on parts, accessories and equipment available in the open market or produces for commercial use not tied or related to IED defeat capabilities	U		Public release and distributions statement A applies.
DD 254s	U - S	Declassify 10 years from date of creation	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.
Statements of work	U - S	Declassify 10 years from date of creation	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies.
Organization Security			
Results of program protection risk management processes / analysis	See Remarks		Mark and handle as FOUO, FOIA exemption 2, 5 applies. Specific information may be derivatively classified from documents such as threat assessments, etc.
Details of specific protection measures associated with the JIEDDO Note: Specific protection measures are those relative to the JIEDDO and not generalized guidance	See Remarks (U-S)		Mark and handle as FOUO, FOIA exemption 2 applies. <u>RAM Measures at a minimum is SECRET</u> Specific information may be derivatively classified from documents such as threat assessments, etc.

FOR OFFICIAL USE ONLY

JIEDDO OPERATIONS

Element	Level	Duration	Remarks
General information regarding the requirements for the JIEDDO and IED defeat systems	See Remarks	Declassify 10 years from date of creation	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Specific technical requirements associated with a specific system, subsystem or component	U-S	Declassify 10 years from date of creation	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Identification of key performance threshold/objective parameters associated with the JIEDDO and specific IED defeat system, subsystem or component	See Remarks	Declassify 10 years from date of this document	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Operational capabilities/shortfalls	See Remarks <u>(U-TS)</u>	Declassify 10 years from date of this document	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 and/or 5 applies.
IED- Related SIGACTS	See Remarks <u>(U-TS)</u>		Classify in accordance with SCG for the program or system. All theater derived SIGACTS are SECRET.
JIEDDO specific tactic's techniques and procedures (TTPs)	See Remarks <u>(C-TS)</u>	Declassify 10 years from date of this document	Classify in accordance with the SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 and/or 5 applies.
JIEDDO CONOPS	U-S	Declassify 10 years from date of this document	Classify in accordance with SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 and/or 5 applies.
Movement of JIEDDO related personnel and equipment.	See Remarks		If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.) If

Formatted: Font: Bold

FOR OFFICIAL USE ONLY

Field team locations	See Remarks		UNCLASSIFIED FOIA 2 potentially applies. If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.).
Field Team Composition, disposition, and strengths	See Remarks	Declassify 10 years from date of this document	If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.). If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2.
Field Team requirements and mission	See Remarks	Declassify 10 years from date of this document	If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.). Specific information not covered in an operational classification guide; classify in accordance with the SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2.
Analysis products by JIEDDO intelligence analysts	See Remarks		Classify in accordance with the applicable Intelligence Community classification guide. If no guidance is available refer to DoDD 5240.06 (DOD CI SCG, December 2005, if UNCLASSIFIED FOIA 2, 4 and 5 applies).
JIEDDO intelligence requirements	S	Declassify 10 years from date of this document	Classify in accordance with current markings or the SCG for the operation, program or system, (if UNCLASSIFIED FOIA 2, 4 and 5 applies).
Specific IED- related system employment locations	See Remarks	Declassify 10 years from date of this document	If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.). (If UNCLASSIFIED FOIA 2, 4 and 5 applies).
Specific IED- related system employment methods	See Remarks	Declassify 10 years from date of this document	If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.). Specific information not covered in an operational or system specific classification; classify in accordance with the SCG for the program or system. Classification of employment locations may be classified a higher levels or within compartmented channels based upon operational guidance.

FOR OFFICIAL USE ONLY

			<p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 and 5 potentially applies.</p> <p>If resulting from combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.).</p> <p>For JIEDDO specific developed lessons learned treat as:</p> <p>Classify in accordance with current classification or the SCG for the program or system.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 and/or 5 applies.</p>
IED lessons learned	U-S	Declassify 10 years from date of this document	<p>Classify in accordance with current classification or the SCG for the program or system.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 and/or 5 applies.</p>
Initial Review Group (IRG) internal decision- making processes and results	U-S	Declassify 10 years from date of this document	<p>Classify in accordance with current markings or the SCG for the operation, program or system.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
Technology Review Group (TRG) internal decision- making processes and results	U-S	Declassify 10 years from date of this document	<p>Classify in accordance with current markings or the SCG for the operation, program or system.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
JIEDD Requirements, Resources and Acquisition Board (JR2AB) internal decision making processes and results	U-S	Declassify 10 years from date of this document	<p>Classify in accordance with current markings or the SCG for the operation, program or system.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
Joint Integrated Product Team internal decision- making processes and results	U-S	Declassify 10 years from date of this document	<p>Classify in accordance with current markings or the SCG for the operation, program or system.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>

C-IED Operational/Intelligence Integration Center (COIC)

For Further Information Refer to Annex A of this Classification Guidance

FOR OFFICIAL USE ONLY

COIC mission	U		
--------------	---	--	--

RED AND BLUE TEAM ACTIONS

Element	Level	Duration	Remarks
Fact that JIEDDO performs red teaming and blue teaming	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Red team and blue team reports	See Remarks		Results are to be classified at the same level as the items or systems being Red Teamed or Blue Teamed – classify in accordance with information revealed. If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as derivative from other sections of this SCG. Classification of red team and blue team plans and results is dependent on the security classification of the information involved.
Field team prototypes of possible new threat modes or techniques	See Remarks		Prototypes without accompanying explanatory information will be handled as FOUO. FOIA 4 potentially applies. When associated with specific Red Team and Blue Team reports classify at the same level as the associated report.
Limitations or vulnerabilities associated with IED defeat systems or subsystems revealed by Red Teaming or technical gaming	See Remarks	Declassify 10 years from date of this document	Classify according to the level of information revealed through the association of limitations or vulnerabilities of specific IED defeat systems. If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as: CONFIDENTIAL if loss of information would reveal or

FOR OFFICIAL USE ONLY

			<p>compromise a future capability.</p> <p>SECRET if details would lead to loss of research, development and engineering; scientific, or technical information that would lead to a tactical disadvantage.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.</p>
--	--	--	---

JIEDDO SYSTEM AND SUBSYSTEM PERFORMANCE AND CAPABILITIES

This section applies to all IED detection and defeat systems and subsystems.

(Many such systems fall under a different Original Classification Authority than JIEDDO owned information – i.e. Warlock Red falls under the authority of PM SW and PEO IEW&S and therefore all classification determinations for this system are found in the Joint counter radio controlled improvised explosive service electronic warfare Program Security Classification Guide) (CREW)

Element	Level	Duration	Remarks
General information regarding the capabilities of IED defeat systems or subsystems	U		General information is that which can be found in unclassified requests for proposals and approved JIEDDO press releases and media guidance, and documents marked with FOIA distribution statement A.
Specific details regarding the capabilities of IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	<p>If system specific classification guidance exists, then classify in accordance with that guidance.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 or 5 applies.</p>
Emerging IED defeat capabilities or systems	See Remarks	Declassify 10 years from date of this document	<p>If system specific classification guidance exists, then classify in accordance with that guidance.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
(CREW) System or Subsystem	See Remarks		<p>For guidance on all CREW system, refer to the Joint Counter Radio Controlled Improvised Explosive Service Electronic Warfare Program Security Classification Guide, 8 August, 2006 (OPNAVINST 5513.8B-8B).</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
Maximum range of detection / defeat for	See Remarks	Declassify 10 years	If system specific classification guidance exists, then classify

FOR OFFICIAL USE ONLY

IED defeat system or subsystem		from date of this document	in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Detection rates	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
The fact that specific IED defeat systems will be used to protect specifically named VIP's	See Remarks (S-TS)	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. The general statement that C-IED systems are used for VIP protection is UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 and/or 5 applies. The fact C-IED systems are being used to protect specific VIPs is classified SECRET based on the program SCG, the loss of information could lead to a tactical disadvantage. Classification of C-IED systems being used to protect specific VIPs may be classified at higher levels or within compartmented channels based upon operational guidance.
Effectiveness of IED defeat systems or subsystems against general threats	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. General categories of threats that C-IED systems are designed to counter (e.g. car alarms, cell phones, etc) UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Effectiveness of IED defeat systems or subsystems against specific threats	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Specific system Concept of Operations (CONOPS)	See Remarks (C-S)	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA

FOR OFFICIAL USE ONLY

			exemption 2, 4 or 5 applies.
Specific system tactics, techniques, procedures (TTPs)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Frequency ranges when expressed in general terms (such as Band A / Band B)	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Frequency bands expressed in general terms that do not reveal actual operating parameters is UNCLASSIFIED.
Frequency bands associated with specific IED defeat systems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. Listing of actual operating frequencies, frequency bands, or entire spectrum coverage is SECRET – the loss of information could lead to a tactical disadvantage. If UNCLASSIFIED, FOIA 4 potentially applies.
Antennas associated with IED defeat systems or subsystems	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. The fact that specific antennas are being used for C-IED systems is UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies. If performance characteristics of an antenna are classified, then classify in accordance with the applicable SCG.
IED defeat system or subsystem reliability, maintainability, and supportability	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Technical details of signal processing or jamming techniques / parameters	See Remarks	Declassify 10 years from date of this	If system specific classification guidance exists, then classify in accordance with that guidance.

FOR OFFICIAL USE ONLY

		document	If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Threat characteristics that are used to determine which IED defeat system or subsystem to employ	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
RF Output power or other information that would reveal effective range of operation	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Input sensitivity or other information that would reveal system or subsystem detection range	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Interoperability between various IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Interoperability between IED defeat systems or subsystems and other equipment (communication equipment, weapons systems, etc)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.

FOR OFFICIAL USE ONLY

JIEDDO RELATED HARDWARE / SOFTWARE

(Some Hardware and Software falls under a different Original Classification Authority than JIEDDO owned information – i.e. Warlock Red falls under the authority of PM SW and PEO IEW&S and therefore all classification determinations for this system are found in the Joint Counter Radio Controlled Improvised Explosive Service Electronic Warfare Program Security Classification Guide)

Element	Level	Duration	Remarks
Technology Integration			
General description of technologies being considered for use by JIEDDO Note: Technologies that have actually been selected for use by JIEDDO are covered in the respective SCG	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as: UNCLASSIFIED - Mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Specific technical details of technologies being considered for use by JIEDDO Note: Technologies that have actually been selected for use by JIEDDO are covered in the respective SCG	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Design Details			
General information regarding IED defeat systems or components of systems	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Design specifications of IED defeat systems or components of systems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Specific technical details regarding IED defeat systems or components of systems (antennas, etc)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance.

FOR OFFICIAL USE ONLY

			If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies. If system specific classification guidance exists, then classify in accordance with that guidance.
Network architecture system view	See Remarks	Declassify 10 years from date of this document	If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Network architecture technical view	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Network architecture network functions	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Software architecture	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Software source code	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Information assurance technical details (To include Cross Domain Guard, Network Intrusion Detection System, Key Fill Bus, firewall, and switches)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Cryptographic capabilities and equipment	See Remarks		Contact OPR COMSEC material and controlled cryptographic items shall be handled, marked and safeguarded in accordance with policies and procedures of the National Security Agency. If UNCLASSIFIED, mark and handle as FOUO, FOIA

FOR OFFICIAL USE ONLY

			exemption 2, 4 or 5 applies.
Modeling and Simulation			
Fact that modeling and simulation is used for design and validation of a specific system, subsystem or component	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as UNCLASSIFIED - Mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Operational parameters for specific modeling and simulation at the force, system, subsystem or component level	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Details of specific items in the modeling and simulation database	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Results of the modeling and simulations	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Commercial Off the Shelf (COTS) / Government Furnished Equipment (GFE)			
Fact that the JIEDDO uses COTS/GFE systems	U		Public Release and Distributions Statement A applies.
Association of COTS/GFE used on a particular IED defeat system, subsystem, or component	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Mark and handle as FOUO, FOIA exemption 4 potentially applies.
Modification of COTS/GFE	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Unusual or unique application of GFE	See Remarks	Declassify 10 years	If system specific classification guidance exists, then classify

FOR OFFICIAL USE ONLY

		from date of this document	in accordance with that guidance.
			If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Technical details about modification of COTS/GFE	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Manufacturing / Fabrications			
Fact that unique / non-traditional manufacturing processes are used to develop IED defeat systems, subsystems, or components	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Technical details of unique / non-traditional manufacturing processes used to develop IED defeat systems, subsystems, or components	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Integration			
Fact that unique / non-traditional integration processes are used to develop IED defeat systems, subsystems, or components	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Identification of unique / non-traditional integration techniques with specific IED defeat systems, subsystems, or components	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Technical details of unique / non-traditional integration techniques relative to IED defeat systems, subsystems, or components	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 3, 4 and 5 applies.
External / Internal Views			
External view of IED defeat systems, subsystems, or components (including	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance.

FOR OFFICIAL USE ONLY

drawings, photographs, etc.)			If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4.
Internal view of IED defeat systems, subsystems, or components (including technical drawings of systems, components such as wiring plans, blueprints, and section cutaways)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Anti-Tamper			
General information regarding the fact that anti-tamper is used on IED defeat systems, subsystems, or components	U		
Technical details regarding implementation of anti-tamper to deter / delay attempts at reverse engineering of hardware / software of IED defeat systems, subsystems, or components	See Remarks		Refer to the Anti Tamper SCG, dated 1 March 2001. If UNCLASSIFIED, FOIA exemption 2, 4 or 5 potentially applies.

VULNERABILITIES AND WEAKNESSES

Element	Level	Duration	Remarks
General information regarding vulnerabilities and limitation of IED defeat systems or subsystems (i.e. information found via open sources related to common vulnerabilities such as the statement that "coalition troops are vulnerable to VBIED attacks")	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. <u>Combination of open source material may classify information</u> General information not covered in a component classification guide is treated as: UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Details of specific operational limitations and vulnerabilities of IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.
Identification of system susceptibilities in the presence of a validated threat to a specific IED defeat system or subsystem	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance.

FOR OFFICIAL USE ONLY

			If UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.
Technical details of specific countermeasure employed (e.g. ECM, Anti-Tamper, Signature Management, etc)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, FOIA, exemption 4 or 5 potentially applies.
Effectiveness of specific countermeasures	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If, UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.
Information regarding signals or initiation means which may not be detected or which may be immune to specific IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If, UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.

INDUSTRY TEST AND EVALUATIONS

Element	Level	Duration	Remarks
Details of IED defeat system or subsystem test plan	See Remarks		Testing is to be classified at the same level as the item being tested – classify in accordance with information revealed. If system specific classification guidance exists, then classify in accordance with that guidance. If, UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.
Identification of specific dates for IED defeat systems or subsystem tests	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Identification of specific test locations associated with IED defeat systems or	U		Mark and handle as FOUO, FOIA exemption 2 applies.

FOR OFFICIAL USE ONLY

subsystems			
Identification of specific or specialized test instrumentation or equipment associated with IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	Classify according to the level of information revealed through the association of specialized test equipment with specific IED Defeat systems. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Predicted test data	See Remarks		Testing is to be classified at the same level as the item being tested – classify in accordance with information revealed. Predicted test data that provides specific performance and capability data on IED defeat System or Subsystem shall be classified in accordance with that component Security Classification Guide. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Raw test data	See Remarks		Testing is classified at the same level as the item being tested – classify in accordance with information revealed. Raw data that provides specific performance and capability data on IED defeat System or Subsystem shall be classified in accordance with that components Security Classification Guide. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Reduced test data	See Remarks		Testing is classified at the same level as the item being tested – classify in accordance with information revealed. Reduced test data that provides specific performance and capability data on IED defeat System or Subsystem components shall be classified in accordance with that components Security Classification Guide. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.

FOR OFFICIAL USE ONLY

TRAINING

Element	Level	Duration	Remarks
Training location specific to the JIEDDO and IED defeat systems, subsystems, or components	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Training that reveals specific system information (e.g. design, development, capabilities, vulnerabilities, etc.) Note: This element includes live training, virtual training, and constructive training.	See Remarks	Declassify 10 years from date of this document	Classify in accordance with the level of information revealed during the training. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Training Aids (Includes both IED training devices and C-IED training devices)	U		If, UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.

MAINTENANCE

Element	Level	Duration	Remarks
Location of specialized maintenance organizations associated with the JIEDDO and IED defeat systems, subsystems, or components	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.
Association of maintenance equipment or tools that may reveal specific system information	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies.
Maintenance that reveals specific system information (e.g. design, development, capabilities, vulnerabilities, etc.)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance.

FOR OFFICIAL USE ONLY

			If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies.
Field level maintenance	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.
Intermediate level maintenance	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.
Depot level maintenance	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.

FOR OFFICIAL USE ONLY

SECTION X - APPLICABLE SECURITY CLASSIFICATION GUIDES

Deputy Secretary of Defense Memorandum Dated 24 Apr 2006, SUBJECT:
Policy on Discussion of IEDs and IED-Defeat Efforts in Open Sources

Operational Capabilities Infusion Team (OCIT) Technology Efforts in Support of
the Detection and Defeat of Improvised Explosive Device (IED) Classification
Guide (Revised 10 March 2004)

MNF-I / MNC-I Security Classification and Marking Guide, Version 5, Change 1,
05 Aug 2005

DoD Security Classification Guide Operation Enduring Freedom, Operation
Noble Eagle, 28 Mar 2002

USCENTCOM Security Classification Guide 0501, Dated: 9 June 2005

Classification Guidance for EC-130H and EA-6B Counter-RCIED Operations in
Operation IRAQI FREEDOM

Classification Guidance for EC-130H and EA-6B Counter-RCIED Operations in
Operation ENDURING FREEDOM

Counter Radio Controlled Improvised Explosive Service Electronic Warfare
Program Security Classification Guide, 8 August, 2006 (OPNAVINST 5513.8B-
88)

FOR OFFICIAL USE ONLY

SECTION XI REFERENCES

1. Executive Order 12958, as amended, 5 Jan 2006
2. AR 380-5, "Department of the Army Information Security Program," 14 Jan 2006
3. DOD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," Jan 1995, Change 1, 31 Jul 1997; Change 2, 28 Feb 2006
4. AR 25-55, "Department of the Army Freedom of Information Act Program," 15 Jan 2006
5. DOD Directive 5230-25, "Withholding of Unclassified Technical Data from Public Disclosure," 6 Nov 1984; Change 1, 8 Apr 1995
6. DOD Directive 5230-24, "Distribution Statements on Technical Documents," 8 Apr 2004
7. DOD Pamphlet 5230.25-PH, "Control of Unclassified Technical Data with Military or Space Application," 15 Apr 2004
8. DOD 5200.1-R "Information Security Program," Feb 2009
9. DOD 5230.9 "Clearance of DoD Information for Public Release," 22 Aug 2008
10. DOD 5230.11 "Disclosure of Classified Military Information to Foreign Governments and International Organizations," 7 Feb 2006
11. DODI 5230.27 "Presentation of DoD-related Science and Technical Papers at Meetings, 6 Oct 1987

UNCLASSIFIED

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)

PFC, U.S. Army,)

HHC, U.S. Army Garrison,)

Joint Base Myer-Henderson Hall)

Fort Myer, Virginia 22211)

Prosecution Objection to
Providing an "Example" Witness
to Examine the Viability of
Reasonable Alternative to Closure

Enclosure 3

3 April 2013

UNCLASSIFIED

End 3 to
APPELLATE EXHIBIT 512
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

Classification Guide Citations by Witness

The Court may find the following classification guide sections particularly helpful in understanding the reasoning behind classification of the information to which the below witnesses will testify and thereby the interests risked if that information is improperly disclosed. This enclosure tracks the witness numbers assigned in the Government's Supplement to Prosecution Response to Scheduling Order: 39a Session on Closure and Motion to Close the Courtroom for Specified Testimony. *See* AE 505. The classified classification guides cited here are provided to the Court *ex parte* via Enclosure 1 of this filing. The unclassified classification guides are provided via Enclosure 2.

1.
 - a. Department of State Classification Guide Subparagraphs IV A, C, D(7), G.
 - b. Defense Counterintelligence and HUMINT Center HUMINT Security Classification Guide I.B and E(1), II.A.
 - c. CENTCOM Security Classification Guide Sections A-2, A-6, A-12.
2.
 - a. Department of State Classification Guide Subparagraphs IV A, G.
 - b. Defense Counterintelligence and HUMINT Center HUMINT Security Classification Guide Sections I.B(36), D, E(2).
4.
 - a. Department of State Classification Guide Subparagraphs IV D(7), G.
6.
 - a. Department of State Classification Guide Subparagraphs IV A, C, D(6), G.
 - b. CENTCOM Security Classification Guide Sections A-2, A-6, A-12.
7.
 - a. Department of State Classification Guide Subparagraphs IV B, D(1)-(2) and (6).
8.
 - a. Department of State Classification Guide Subparagraphs IV B, D.
9.
 - a. Department of State Classification Guide Subparagraphs IV A, C, D(7), G.
 - b. Defense Counterintelligence and HUMINT Center HUMINT Security Classification Guide Sections I.A, B, E(1).
 - c. CENTCOM Security Classification Guide Sections A-2, A-6, A-12.
10.
 - a. Department of State Classification Guide Subparagraphs IV C, D.
12.
 - a. Department of Defense Offensive Counterintelligence Operations Procedures and Security Classification Guide T2(26)
13.
 - a. Department of State Classification Guide Subparagraph IV G.
14.
 - a. CENTCOM Security Classification Guide Sections A-3, A-6, A-13
 - b. Security Classification Guide for Joint Improvised Explosive Device Defeat Organization page 22, 23.
15.
 - a. Department of State Classification Guide Subparagraphs IV A, D(2) and (5).

- b. CENTCOM Security Classification Guide Sections A-6, A-7, A-12.
- 16. a. Department of State Classification Guide Subparagraphs IV B, E.
- 17. a. Department of State Classification Guide Subparagraphs IV A, C.
b. CENTCOM Security Classification Guide Sections A-2, A-6, A-7, A-12.
- 19. a. Department of State Classification Guide Subparagraphs IV B, D.
- 20. a. CENTCOM Security Classification Guide Sections A-2, A-12.
- 21. a. Department of State Classification Guide Subparagraphs IV B, D.
- 23. a. Department of State Classification Guide Subparagraphs IV A, B, D, G.
- 26. a. Department of State Classification Guide Subparagraphs IV A, B, D.
- 27. a. Department of State Classification Guide Subparagraphs IV A, B, D, E, G.
- 28. a. Department of State Classification Guide Subparagraphs IV A, B, D.

Appellate Exhibit 512

Enclosure 4

33 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 512

Enclosure 5

33 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

UNCLASSIFIED

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)

PFC, U.S. Army,)

HHC, U.S. Army Garrison,)

Joint Base Myer-Henderson Hall)

Fort Myer, Virginia 22211)

Prosecution Objection to
Providing an "Example" Witness
to Examine the Viability of
Reasonable Alternatives to Closure

Enclosure 6

3 April 2013

UNCLASSIFIED

Encl 6 to
APPELLATE EXHIBIT 512
PAGE REFERENCED:
PAGE OF PAGES



[alexabrien.com](#) | [blog](#) | [interviews](#) | [audio](#) | [video](#) | [features](#) | [about](#) | [in the press](#) | [contact](#) | [archives](#) | [time line](#) | [redacted names and notables](#)

Redacted Names and Notables

csv file in unallocated space of the Dell 40 that could not be tied to a user profile of dated that contained 5 columns. Unique Number Data the cable was published to the Department of State server, Message Record Number (MRN) Classification; Base64 encoding. Special Agent David Shaver Computer Crimes Investigation Command (CCIU) testified that he was able to decode the Base64. No evidence the information was passed to an unauthorized person

10000 CIDNE (Rehman says 10000; transcriber says 100000) documented findings and reports in the unallocated space of the SD card allegedly obtained at the second search of Debra Van Aalstine Bradley Manning's aunt home after having allegedly been shipped from Iraq in October 2010

12 pages of Brady materials from interim damage assessments from November 2010 by the Federal Communications Commission the Federal Trade Commission the U.S. Department of Urban Development the Millennium Challenge Corporation the National Archives and the United States Marshals Service Some of these interim damage assessments reference investigations by ONCIX and DIA. For reference the 26 November 2010 "Memorandum for the Office of the National Counterintelligence Executive (ONCIX) the Federal Communications Commission states "As requested this Memorandum provides the response of the Federal Communications Commission (FCC) as requested by the NCIX memo dated 26 October 2010" Similarly the 19 November 2010 letter from the U.S. Department of Housing and Urban Development is addressed to the DIA. Moreover the DIA is overseeing the Information Review Task Force an investigation into the alleged disclosures Further the interim damage assessments also reveal the Office of the Director of National Intelligence (ODNI) has relevant investigative files See letter from United States Marshals "On October 13 2010 the Office of the Director of National Intelligence (ODNI)... provided a checklist of questions that it recommended each agency impacted by [W] dissemination use to assess the impact on its operations"

14 hard drives from PFC Manning T-SCIF

14 hard drives from PFC Manning T-SCIF Government "Encase forensic images requested by Defense is within Department of Defense (DOD) but it is classified. Some factual showing for materiality total drives. The unit redisplayed July 2010 and pulled from the redeployment all computers with a user profile of Bradley Manning. Any of those drives they collected. Then the unit was free to discard and DV all the procedures post deployment any additional drives in September 2010. Defense request to preserve Encase was made in September 2011 when the unit was down range. Keeps all theater equipment. We notified Army CID

166 charged documents from the Department of State (State Department) (DoS)

17 April 2012 Memorandum for Principal Officials of Headquarters Department of the Army "[i]t was only recently determined that no action had been taken by HODA pursuant to the 29 July 11 memo from DOD (Department of Defense) OGC (Office of the General Counsel)"

2007 Apache Airstrike (Collateral Murder)

2008 PowerPoint Presentation (PPT) for corrective training on infocsec. How to handle it; if you are a person with access... how it could be dangerous. There are sources looking for info on military Different types: foreign governments enemies spies and hackers

2012 \$1 to \$2 Million forecasted contracting opportunity for the FBI in Fairfax VA for "WikiLeaks Software and Hardware" for incumbent contractor ManTech dated November 7 2011

22.225.41.22 (22) Alienware S1PRNet computer Bradley Manning shared at the T-SCIF workstation with Sergeant Chad Madaras

22.225.41.40 (40) Dell S1PRNet computer Bradley Manning shared at the T-SCIF workstation with Sergeant Chad Madaras

247 WikiLeaks Working Group

2703(d) Orders

35F or 35 Fox

63 agencies and other organizations the Government has claimed to have contacted

706 Board

72 addresses in the unallocated space of Manning's MacBook Pro that reference to a Thunderbird email cache

72.66.112.117 resolved to Verizon Communications and was connected to the account of Bradley Manning's aunt Debra Van Aalstine

84 emails provided to defense by the Government

84 Quantico emails that Ashton Fen sent on the evening of 26 August (after the Defense's attachments had already been sent) at 19:50 which reveal that the senior Brig officer who ordered PFC Manning to be held in MAX and in POI was receiving his marching orders from a three-star general

88.80.17.76 resolves to PRQ (PerQuito AB) an ISP based in Sweden

94 authorized programs for Distributed Common Grounds System - Army (DCGS-A) computer

a copy of Collateral Murder as it was released on the WikiLeaks.org website and also what appeared to be the source file in the unallocated spaces of the Alienware 22 computer. The first instance of this was March and was found through restore points using Encase

a removable 500 GB hard drive from Adrian Lamo's Linux machine mobile laptop

A self-portrait Manning took with a camera held in one hand standing in front of a mirror in the basement of his aunt's Debra Van Aalstine's house on 26 January 2010 in the unallocated space of an SD card allegedly obtained at the second search of Debra Van Aalstine Bradley Manning's aunt home after having allegedly been shipped from Iraq in October 2010

a) Military Organizations/Entities: Army Criminal Investigation Command (CIC) Defense Intelligence Agency (DIA) Defense Information Systems Agency (DISA) CENTCOM SOUTHCOM

Acceptable Use Policy (AUP)

Acceptable Use Policy (AUP) for the Alienware 22 and Dell 40 machines

According to the 2 December 2011 Defense Request for Article 32 Witnesses and the Article 32 Patrol Hearing testimony of Special Agent Calder/Robertson CCIU SA Robertson extracted the hard drives from the two S1PR and one S1PR computers collected from the T-SCIF: the personal laptop of Staff Sergeant Peter Bigelow Supply Room and the personal external hard drive of PFC Manning. According to the 15 March 2011 Article 32(a) Session despite Army Criminal Investigative Command's (CIC) own preservation request for other hard drives from the T-SCIF in September 2010 and the defense preservation request for the same in September 2011 the Government notified the Court and defense that of the 181 drives identified by the Government as part of the Second Engage Combat Team 10th Mountain Division only computers with a user profile for Bradley Manning were preserved. The other computers the Government said the unit was free to discard and DV all the procedures post deployment in September 2010. The Government was able to identify 14 other computers post deployment from the T-SCIF by serial numbers but the Government said that of those 14 drives two drives were completely inoperable seven drives were wiped and one drive was partially wiped

According to the evoking US Government unauthorized access theory USG alleges Pfc. Manning placed Wget on "two separate systems" 1030(a)(1)

According to the Office of the Director of National Intelligence (ODNI) 4.2 million federal employees contractors and consultants have security clearances for SECRET information

Adium contact list in the allocated space of Bradley Manning's MacBook Pro

Adrian Lamo

Adrian Lamo contacted Special Agent Antonio Patrick Edwards Army Computer Crimes Investigation Command (CCIU)

Adrian Lamo contacted us and related that he became aware on the Internet of someone that he did not know who was part of the original decryption effort on the Garani video who worked for Department of Energy (DOE) who he later said was Jason Katz

Adverse administrative or UCMJ actions

Afghanistan occurring on or about 4 May 2009. "The Defense requests that the Government identify the exact number and specific records it believes supports this specification for the Defense's review." Prosecution Answer: 13 records.

After oral argument on 21 March 2012 the Court asked the Government to respond inter alia to the following question Is there any favorable material [in the damage assessments the Government has reviewed]? The Government's response with respect to the Defense Intelligence Agency (DIA) and Information Review Task Force (IRTF) reviews was that there was favorable material. The concession that the damage assessment is favorable is wholly at odds with the Government's statement two weeks earlier in its Response to Defense Motion to Compel Discovery (No. 1)

Air Force Intelligence

AIR Special Agent Tom Graham Army Criminal Investigation Command (CID) had produced (ref number: 00000184-190)

Al-Qaida

Al-Qaida in the Arabian Peninsula (AQAP)

alleged Adium chat logs in XML format on Bradley Manning's MacBook Pro between "dawnetwork@jabber.ccc.de" and "pressassociation@jabber.ccc.de" who Mark Johnson ManTech International Contractor reports to Special Agent David Shaver Army Computer Crimes Investigative Unit (CCIU) says is Julian Assange aka Nathaniel Frank but later admitted had no evidence of a connection between Bradley Manning and a known WikiLeaks associate

alleged Adium chat logs on Manning's Apple MacBook Pro in XML format between "bradass87" and Adrian Lamo

alleged AIM chat logs on Adrian Lamo's HP Windows mini laptop or Netbook that had a hard drive in it that belonged to Adrian Lamo

alleged chat log as published by Wired on 13 July 2010

alleged chat log excerpts as published by Wired on 10 June 2010

alleged chat logs between Adrian Lamo and bradass87

alleged chat logs between Adrian Lamo and Danny Clark provided to Special Agent Antonio Patrick Edwards CCIU by Adrian Lamo

alleged May 11 2010 to May 19 2010 email chain between Bradley Manning and Eric Schmidt: "I was the source of the 12 Jul 07 video of the Apache Weapons team which killed the two journalists and injured two kids"

Almanza denied one agent the defense requested who was on the prosecution's original witness list dated July 7 2010. The defense requested the "attendance of XXXXXXXXXX in order to provide the Investigating Officer with testimony concerning the joint investigations being conducted by both the Department of State and the Federal Bureau of Investigation

Almanza is Facebook friends with John N. Maher Deputy General Counsel for Contracting at the Defense Intelligence Agency

also reveal that the senior Brig officer former Security Battalion Commander Col. Robert G. Oltman who ordered PFC Manning to be held in MAX custody and Prevention of Injury at Quantico indefinitely was receiving his marching orders from Joint Chiefs Chairman General Martin Dempsey's deputy Lt. General George J. Flynn a three star General Director J-7 Joint Staff

Although Wiget was not apparently officially authorized for the individual user it was authorized for use on the Army Server components of the system As such Wiget is a program that is authorized to be used on certain military computers

and 2/10 Mountain. Identified 181 hard-drives. And out of those serial numbers 13 hard drives that were in the SCIF when the unit was deployed. CID had one other drive. We had not given to Defense because it is classified. Would have to be reviewed by OCA. Then authority granted to turn over based on if you rule it is relevant and necessary. Based on your ruling we will get the approval for MRE 505"

and Reconnaissance (AF ISR)

Any damage assessment by one of the 63 agencies to the Office of the National Counterintelligence Executive (ONCE) in the Office of the Director of National Intelligence (ODNI)

Appellate Exhibit CXXXIX at 9 The Government has indicated albeit cryptically its Wiget theory for the information covered by Specification 13 of Charge II

Army 15-6 Investigation

Army Computer Crime Investigative Unit (CCIU) obtained chats from Mr. Adrian Lamo and collected computer belonging to Mr. Adrian Lamo

Army Computer Crimes Investigative Unit (CCIU)

Army Counterintelligence Center (ACIC)

Army Counterintelligence Center (ACIC) logs

Army Criminal Investigation Command (CID)

Army Criminal Investigation Command (CID) and the Federal Bureau of Investigation (FBI) obtained a federal warrant to search and did a search of Jason Katz's government work station

Army Criminal Investigation Command (CID) investigative files

Army Criminal Investigation Command (CID) The primary law enforcement organization within the Department of the Army focused on investigating the accused [Manning]

Army Criminal Investigation Command (CID) two (2) investigations US Forces Iraq (USFI) and 1st Armored Division (1st AD)

Army Knowledge Online

Army Regulation 25-2 dated 24 October 2007

Army Regulation 27-26 Rules of Professional Conduct for Lawyers

Army Regulation 380-5 dated 29 September 2000

Army Regulation 380-5 dated 29 September 2000 Paragraphs 1-21 and 6-1

Army Regulation 380-5 dated 29 September 2000 Paragraphs 1-21 and 6-1

Article 104 aiding the enemy

Article 121 Larceny and Wrongful Appropriation

Article 13

Article 13 Judge rules on recent review of 600 Quantico emails all but 12 material to preparation of defense

Article 13 of the Uniform Code of Military Justice states: "No person while being held for trial may be subjected to punishment or penalty other than arrest or confinement upon the charges pending against him nor shall he arrest or confinement imposed upon him be any more rigorous than the circumstances required to insure his presence but he may be subjected to minor punishment during that period for infractions of discipline"

Article 134 General article

Article 15 (Non-judicial Punishment)

Article 3 Judge's Protective Order

Article 31

Article 37 President Obama declares Pfc. Manning guilty before trial

Article 37 Unlawful Command Influence

Article 92 Failure to obey order or regulation

ARTFACT - naming of a CD that Special Agent David Shaver Computer Crimes Investigation Command (CCIU) burned. Computer BD-RE Drive (D:) 100527_0357 Organize - Burn to disk. It is unclear on which computer Special Agent David Shaver Computer Crimes Investigation Command (CCIU) made this disk image to use in his testimony

As a result of the Government's inconsistent positions on this issue this Court ordered the Government to produce a witness from the Department of State (State Department) (DoS) to appear at the oral motions argument to confirm what information is or is not available within that agency

Assistant Secretary of the Navy Juan M. Garcia

at 15 March 2012 Article 39(a) session Fein: The Enclave forensic images of hard drives in TSCIF. Government did identify some drives that have not been turned over because they were used in a classified TSCIF. So they are considered classified

at 15 March 2012 Article 39(a) session Government said it would not be invoking MRE 505 for classified discovery. Consider at THAT time Government was suggesting an August 2012 trial calendar and had NOT scheduled any MRE 505 into original proposed trial calendar (it has NOW has invoked MRE 505)

at 15 March 2012 Article 39(a) session Judge Lind said "This case deal with classified information. There are over three million pages of documentation in this case"

At the 18 October 2012 Article 39(a) Session Judge Lind ruled that the Court would take Judicial Notice of the President's 27 July 2010 statement from the Rose Garden and published on the White House Web site on the lack of damage from the release of the Afghan War Logs for use during the sentencing portion of the trial - since actual damage is precluded from the trial on the merits without the Court's permission - because the President's statement is made by a "party opponent" to the accused in United States v. Pfc. Bradley Manning is a statement of fact the statement was likely checked by the Government before it was given was given to the press with the intention of wide dissemination to the public and the President's statement had the "hallmarks of a testimonial statement"

At the 18 October 2012 Article 39(a) Session the Government revealed that in the Spring and Summer of 2011 military prosecutors were coordinating with the Department of Justice and the FBI for the release of information related to the US investigation of WikiLeaks Assange and other civilians for the military prosecution of Pfc. Manning. In a 22 May 2011 memo to the Special Convening Authority Col. Carl R. Coffman Jr. Commander of Joint Base Myer seeking an executable delay the military prosecutors said they were dealing with "sealed search warrants and subpoenas and Grand Jury material in the federal courts" (plural). In a 21 June 2011 memo to Col. Coffman - a period documented in the public record for known subpoenas search warrants and testimony by the Grand Jury in the Eastern District of Virginia investigating WikiLeaks for "conspiracy to communicate or transmit national defense information in violation of 18 USC 793(g) and conspiracy to violate the laws of the United States in violation of 18 USC 371 to wit knowingly accessing a computer without authorization or exceeding authorized access and having obtained information protected from disclosure for reasons of national defense or foreign relations in violation of 18 USC 1030(a) and knowingly stealing or converting any record of thing of value of the United States or any department or agency thereof in violation of 18 USC 641" - the military prosecutor requested an executable delay because among other matters "another document was 'discovered'". military prosecutors noted that they were dealing with the Government at the 18 October 2012 Article 39(a) Session when the investigation was completed the Government answered "The investigation is not complete. The investigation is still ongoing." On 30 June 2012 Department of Justice spokesperson Dean Boyd confirmed in like manner to the military prosecutor to Judge Lind "There continues to be an investigation into the WikiLeaks matter." In their 25 July 2011 memo to Col. Coffman requesting more delay the military prosecutor wrote that another "document" that was "discovered" By June 25 July 2011 another document became two "certain sensitive documents" that were "identified separately." The military prosecutor also said that it was relying on "US Attorneys" (plural) to "keep things moving in the US District Courts" (plural). In a 25 August 2011 memo to Col. Coffman requesting more delay the military prosecutor said they were waiting for the FBI and the Diplomatic Security Services (DSS) to disclose "portions" of their investigative files "relevant" to Manning's defense. In a 26 September 2011 memo to Col. Coffman requesting more delay the military prosecutor said that it had "obtained all authorizations and signed protective orders from the federal Courts" and that the Government had obtained the "portions" of the FBI and Diplomatic Security Services file "relevant" to Pfc. Manning to give to the defense.

Attorney General Eric Holder

aymond G. McGrath director of the Office of Counterintelligence and Consular Support in the Bureau of Intelligence and Research at the Department of State (State Department) (DoS)

b) Joint Investigations: Federal Bureau of Investigation (FBI) Diplomatic Security Services (DSS) at the Department of State (State Department) (DoS)

b.zip placed on linux work computer of Jason Katz on 15 December 2009 and BE22PAX.wmv video file evidence of a cracking program being downloaded and installed on linux work computer of Jason Katz

backup.xls

bash history evidencing cracking program was trying to decrypt b.zip on the linux work computer of Jason Katz

Bates # 00124331 (forensic report indicating that the keyword "tcoland" was searched for a total of fourteen times from both of PFC Manning's primary and secondary SIPRNET computers)

Ben Rhodes the Deputy National Security Advisor for Strategic Communications

Bill of Particulars

Bill of Particulars "How did PFC Manning 'knowingly' exceed authorized access on a Secret Internet Protocol Router Network computer in Specification 13 [and 14] of Charge II?" Government disputed answering this in the Bill of Particulars. In the discussion with the Court the Government said in response "Manning had name and password. On the certain occasion that he obtained these documents he was exceeding authorized access... which would be a usage based"

Bill of Particulars "How did PFC Manning knowingly give intelligence to the enemy?" Prosecution Answer: Indirectly through the WikiLeaks Web site.

Bill of Particulars "If the government is alleging that PFC Manning stole purloined and converted the charged items does each theory of culpability apply equally to every charged item?"

Bill of Particulars "In Specification 1 [Charge I] what is the alleged conduct that the Government believes was an attempt to bypass network or information system security mechanisms?"

Bill of Particulars "In Specification 10 [Charge II] the Government alleges "more than five classified records relating to a military operation in Farah Province

Bill of Particulars "In Specification 13 the Government alleges "more than seventy-five classified United States Department of State cables...". The Defense requests that the Government identify the exact number and specific records it believes supports this specification for the Defense's review." Prosecution Answer: 16 records

Bill of Particulars "In Specification 2 and 3 [Charge III] how is the Government alleging the software was added to the computers?" Government disputed answering this question. The Judge did rule that she would not add it to the Bill of Particulars because Defense had access to the expert and forensics. See Court discussion. Government said in response that they don't "think" they know how the software was added "But we do know that it was physically present on the computer" Government also said [Bates No. 00211037 is the forensic evidence that alleged that the Government alleges shows Pfc. Manning added unauthorized software Wget to his primary computer Alienware 22.225.41.22 SIPRNet (22) computer

Bill of Particulars "In Specification 2 and 3 [of Charge III] which computer is the Government alleging the software was added to?" Prosecution: 22.225.41.22... on SIPRNet"

Bill of Particulars "In Specification 3 [Charge II] the Government alleges "more than one classified memorandum produced by a United States Government intelligence agency...". The Defense requests that the Government identify the exact number and specific records it believes supports this specification for the Defense's review."

Bill of Particulars "In Specification 4 [Charge III] how does the Government allege PFC Manning used an information system in a manner other than its intended purpose?" Prosecution Answer: "Downloaded Global Address List using SIPRNet."

Bill of Particulars "In Specification 5 [Charge II] the Government alleges "more than twenty classified records from the Combined Information Data Network Exchange Iraq database...". The Defense requests that the Government identify the exact number and specific records it believes supports this specification for the Defense's review." Prosecution Answer: 52 records.

Bill of Particulars "In Specification 7 [Charge II] the Government alleges "more than twenty classified records from the Combined Information Data Network Exchange Afghanistan database...". The Defense requests that the Government identify the exact number and specific records it believes supports this specification for the Defense's review." Prosecution Answer: 37 records.

Bill of Particulars "In Specification 9 [Charge II] the Government alleges "more than three classified records from a United States Southern Command database...". The Defense requests that the Government identify the exact number and specific records it believes supports this specification for the Defense's review." Prosecution Answer: 5 records.

Bill of Particulars "In what manner did PFC Manning wrongfully and wantonly cause intelligence to be published on the internet?"

Bill of Particulars "What 'intelligence' is the Government alleging PFC Manning gave to the enemy?"

Bill of Particulars "What was the 'indirect' means allegedly used in order to aid the enemy?" Prosecution Answer: WikiLeaks Web site

Bill of Particulars "What was the 'indirect' means allegedly used in order to aid the enemy?" The Government also stated that its theory of indirect means was that PFC Manning gave the charged intelligence to the WikiLeaks website

Bill of Particulars "Who is the alleged enemy?" Prosecution Answer: The Government has further clarified that the "enemy" to whom PFC Manning allegedly indirectly gave intelligence is Al-Qaida Al-Qaida in the Arabian Peninsula and an entity specified in Bates Number 00410660 through 00410664

Bill of Particulars [Missed Defense Question] Prosecution Answer: "Accused attempted FTP USER Account Password"

Bill of Particulars "What specific theory of culpability does the Government intend to rely upon? In other words does the Government allege that PFC Manning 'stole' 'purloined' or 'converted'?" Government said they would get to that in instructions and that the Government considered "steal and purloin" as the same thing.

Birgita Jonsdottir

Birgita Jonsdottir Twitter

Bradley Manning does not have access to classified information in his own case under the Court Protective Order

Bradley Manning Email Account

Bradley Manning email accounts: Google Gmail, .mil, email for Brianna Manning

Bradley Manning Facebook Account

Bradley Manning or Brianna Manning Email: .mil - Google

Bradley Manning Twitter Account

Bradley Manning was on the 'Shia threat' team according to Captain Steven Lim 2nd Brigade Military Intelligence (MI) Company Commander Brigade S2

Bradley Manning's Amazon Account

Bradley Manning's Apple MacBook Pro

Bradley Manning's Dad

Bradley Manning's Google Account

Brady

Brianna Manning or Gender Identity Disorder
Brigade Commander

Brigade S2 is the Official Classification Authority for classification review of the unclassified July 12 2007 Baghdad airstrike videos also known as "Collateral Murder"

Bureau of Intelligence and Research

Bureau of Intelligence and Research at the Department of State (State Department) (DoS)

but I am guessing

By February 16 2012 the Government had provided approximately 78148 pages of unclassified discovery to the Defense and approximately 333194 pages of what the Government considers classified discovery. The vast majority of this discovery however is not responsive to the specific items repeatedly requested by the Defense

c) Closely Aligned Organizations: Department of State (State Department) (DoS) Department of Justice (DoJ) Government Agency (Central Intelligence Agency CIA) Office of the Director of National Intelligence (ODNI) Office of the National Counterintelligence Executive (ONCIX)

Cached version of the WGET version 1.11.4 download Web page on the NIPRNET computer that included a profile for Bradley Manning

Camp Anjan Kuwait

Camp Liberty Iraq

Captain Angel Overgaard military prosecutor in US v Pfc. Manning

Captain Barclay Keay S2X

Captain Barclay Keay testified that he deployed to Iraq with the 2nd Brigade Combat Team (2nd BCT) 10th Mountain Division (10 MTN) in November of 2009 which had already deployed earlier in October 2009 to Iraq. Keay testified testified that his first deployment was in S2 or Intelligence. S2 refers to 'Company' level intelligence. Keay testified that initially he did not have an specific intelligence position but that he was the T-SCIF night-shift OIC [Officer in Charge] his first three weeks. Keay testified that his job was S2X. According to GlobalSecurity.org "S2x is the intelligence staff officer for HUMINT [Human Intelligence] and CI [Counterintelligence] activities. The S2x provides focus and technical support for all CI [Counterintelligence] and HUMINT [Human Intelligence] activities. He ensures the collection analysis and dissemination of HUMINT [Human Intelligence] and CI-related [Counterintelligence] intelligence and information is in concert with the commander's critical information requirements." Keay testified that during the night-shift he supervised three soldiers: Sergeant (former Specialist) Daniel Padgett Pfc. (former Specialist) Bradley Manning and (now) Keay testified that Padgett Manning and Cooley took over the task left to them by the day-shift. Keay testified that he believed that a NCOIC [Non Commissioned Officer in Charge] was not with him on the night-shift because "there wasn't enough going around" and that the primary focus was on the day-shift when most of the intelligence "was happening". Keay testified that after three weeks as the OIC [Officer in Charge] of the night-shift he was moved to the day-shift.

Captain Brian Moore Defense Forensic Psychiatrist

Captain Casey Martin (married name Fulton) Platoon leader and Brigade Assistant S2 Officer

Captain Casey Martin (married name Fulton) Platoon leader and Brigade Assistant S2 Officer considered mIRC and Google Earth to be baseline authorized applications

Captain Casey Martin (married name Fulton) Platoon leader and Brigade Assistant S2 Officer said main focus was election security in March 2010 before that it was to disrupt enemy operations

Captain Casey Martin (married name Fulton) Platoon leader and Brigade Assistant S2 Officer says it was ok if people played pirated versions of movies they purchased from Iraqi nationals on their workstations in the T-SCIF

Captain Casey Martin (married name Fulton) Platoon leader and Brigade Assistant S2 Officer says main focus was election security in March 2010 before that it was to disrupt enemy operations

Captain Casey Martin (married name Fulton) Platoon leader and Brigade Assistant S2 Officer says she had a verbal conversation with Bradley Manning about the Jul 2007 Baghdad Apache airstrike (known later as Collateral Murder) and then Bradley Manning sent her an email with a side by side video comparison

Captain Casey Martin (married name Fulton) Platoon leader and Brigade Assistant S2 Officer says she saw Bradley Manning curled in a ball on the floor with Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action)

Captain Casey Martin (married name Fulton) Platoon leader and Brigade Assistant S2 Officer says the reason for the ability to burn CDs was to share information with Iraqis. It was part of the mission

Captain Casey Martin (married name Fulton) Platoon leader and Brigade Assistant S2 Officer says the person responsible for DEROG's was 1st Lt. Elizabeth Fields or Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action)

Captain Casey Martin (married name Fulton) Platoon leader and Brigade Assistant S2 Officer was not in Bradley Manning's chain of command her relationship with Manning was merely counseling

Captain Hunter Whyte military prosecutor in US v Pfc. Manning

Captain James Morrow military prosecutor in US v Pfc. Manning

Captain James Morrow: Your Honor The Government would maintain that PFC Manning had a user name and a password to a SIPRNET computer while deployed. On certain occasions when he accessed that computer for certain you know to obtain these documents he was exceeding authorized access. I can't - there is no means. I mean there is no - I don't think it's - a mystery how he got onto the computer. I think Mr. Coombs is focusing on the [inaudible] diplomacy aspect of it when the focus should be on when he access [sic] the computer to do certain things

Captain John Haberlat a spokesman for the Military District of Washington (MDW)

Captain Joshua Tooman military defense US v Pfc. Manning

Captain Matthew W. Freeburg after Pfc. Manning's alleged assault of Specialist Jihreah Showman on May 7 2010 Captain Matthew W. Freeburg "removed Pfc. Manning from the T-SCIF and sent him to work in the Supply Room." See Staff Sergeant Bigelow's testimony for more information. Captain Matthew W. Freeburg then "gave PFC Manning an Article 15 (Non-judicial Punishment) [reducing him from SPC (Specialist) to PFC (Private First Class)]."

Captain Matthew W. Freeburg became Company Commander of Headquarters and Headquarters Company 2nd Brigade Combat Team 10th Mountain Division in April or May of 2010 towards the end of the 2nd Brigade Combat Team 10th Mountain Division's deployment and a month of so before Pfc. Manning's arrest at FOB Hammer Iraq. According to Captain Steven Lim's testimony

at the Article 32 Preliminary Hearing the situation was one of at least two publicly known command changes in the 2nd Brigade Combat Team 10th Mountain Division during deployment which Captain Lim testified was atypical since command rarely changes during deployment.

Captain Matthew W. Freeburg Company Commander of Headquarters and Headquarters Company 2nd Brigade 10 Mountain Division

Captain Matthew W. Freeburg was the "property book holder for all the computers within HHC (Headquarters and Headquarters Company) 2BCT [Second Brigade Combat Team 10th Mountain Division]." According to defense's account of Captain Freeburg's sworn statement Captain Freeburg provided the "commander's authorization to seize and search the computers PFC Manning was known to work on. [Captain Freeburg] also provided search authorization to search PFC Manning's room."

Captain Matthew W. Freeburg's sworn statement based on recommendations by [UNIDENTIFIED MENTAL HEALTH PROFESSIONAL(S)] Captain Freeburg "believed it was shocking that something more serious had not been done to address PFC Manning's behavioral issues prior to him assaulting [Specialist Jihfeah Showman] and receiving Article 15 [Nonjudicial Punishment]."

Captain Matthew W. Freeburg's sworn statement Captain Freeburg "went to [AN UNIDENTIFIED MENTAL HEALTH PROFESSIONAL] at Behavioral Health to discuss PFC Manning's condition. [AN UNIDENTIFIED INDIVIDUAL] told [Captain Freeburg] that PFC Manning's troubles were deeper than the Army could fix and that [Pfc. Manning] should be separated." Further Captain Freeburg "sent PFC Manning to an [UNIDENTIFIED MENTAL HEALTH PROFESSIONAL] for an evaluation."

Captain Ogletree at Fort Huachuca

Captain Paul Bouchard military defense US v Pfc. Manning

Captain Steven Lim 2nd Brigade Military Intelligence (MI) Company Commander Brigade S2

Captain Steven Lim 2nd Brigade Military Intelligence (MI) Company Commander Brigade S2 counseled [Lt. General Robert L.] Caslen that he only learned about the email that Bradley Manning sent to sent to Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) with a photo of himself dressed as a woman after Manning was apprehended

Captain Steven Lim 2nd Brigade Military Intelligence (MI) Company Commander Brigade S2 gave the analyst link to Net Centric Diplomacy database through email with no password required in January 2010. Got from headquarters. Headquarters said for Captain Steven Lim 2nd Brigade Military Intelligence (MI) Company Commander Brigade S2 to pass along

Captain Steven Lim 2nd Brigade Military Intelligence (MI) Company Commander Brigade S2 replaced Major Cliff Clausen who could not explain to the commander in the way the commander needed in January 2010

Captain Steven Lim 2nd Brigade Military Intelligence (MI) Company Commander Brigade S2 says US Forces Iraq partnered with Iraq 2nd Brigade was authorized to release that information to Iraq defense forces because that was part of their mission to train the Iraqis how to use information and to share information with Iraqis

Captain Thomas Cherepko

Captain Thomas Cherepko received a letter of admonishment from Lt. General Robert L. Caslen for "failure to ensure brigade was properly certified" in March of 2011

Captain Thomas Cherepko says that the DAIG (Department of the Army Inspector General) did not perform an inspection until late in deployment

Captain Thomas Cherepko secured some network logs which are official communications between computers for Special Agent Calder Robertson CCIU

Captain Thomas Cherepko tasked one of his soldiers with doing the forensic imaging either Sergeant Joseph Benhail or Private Dody Cherepko could not remember which

Captain William Hoder Quantico Brig Forensic Psychiatrist

Captain William Hoder Quantico Brig Forensic Psychiatrist recommended on 27 August 2010 that I be taken off of POI watch and that my confinement classification be changed from MAX to Medium Custody in (MCI)

Catherine Brown

CD collected from in Bradley Manning's Containment Housing Unit (CHU) that had been marked SECRET

CD was found in Bradley Manning's Containment Housing Unit (CHU) that had been marked SECRET

CENTAUJ logs also known as NetFlow logs for the period 1 October 2009 to end of May 2010 collected from the Office of the Director of National Intelligence (ODNI) for the IP addresses 22.225.41.22 and 22.225.41.40 associated with the Dell 40 and Alienware .22 machines respectively. These track date time and packet information

CENTCOM

CENTCOM Server

CENTCOM Server Farah Investigation Folder created in May 2010 "video" folder BE22PAX.zip created in May 2009 Three (3) videos that Shaver said he found in the CENTCOM Farah investigation folder. [Defense mentions this on cross-examination]

CENTCOM server logs

CENTCOM server logs. CENTCOM server logs do not record external IP address. They track date time and file(s) requested. CENTCOM logs evidence only one PowerPoint file "Farah brief final version" was downloaded by the Alienware .22 computer on 10 April 2010 at 13:12:24 hours. Since CENTCOM logs do not track IP addresses this statement pertaining to the Alienware computer associated with the .22 IP address by Shaver needs further elucidation

Center for Constitutional Rights (CCR) extraordinary writ filed in this case with the Court of Appeals

Central Intelligence Agency (CIA) (Government Agency)

Central Intelligence Agency (CIA) (Government Agency) forensic results or investigative files

Central Intelligence Agency (CIA) (Government Agency) Red Cell Special Memorandum "Afghanistan: Sustaining West European Support for the NATO-led Mission—Why Counting on Apathy Might Not Be Enough"

Central Intelligence Agency (CIA) (Government Agency) The accused [Manning] is charged with compromising Government Agency's (Central Intelligence Agency CIA) documents and the Government intends to use additional information from the Agency during its case-in-chief

Central Intelligence Agency (CIA) Wikileaks Task Force (WTF) damage assessment

Central Intelligence Agency (CIA) Wikileaks Task Force (WTF) damage assessment (Second Damage Assessment)

Central Intelligence Agency (CIA) World Intelligence Review (WIR) Logs

Central Intelligence Agency (Government Agency) Red Cell Memoranda

CHAIN OF COMMAND Col. David M. Miller Commander of the Second Brigade Combat Team (2BCT) 10th Mountain Division (10 MTN) was the most senior officer Pfc. Manning's chain of command within the 2nd Brigade Combat Team 10th Mountain Division

Chairman of the Joint Chiefs of Staff formerly Admiral Mike McMullen

Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey

Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey who like the President declared Pfc. Manning guilty before trial

Chet Usher

Chet Usher sent an email to Special Agent Antonio Patrick Edwards Army Computer Crimes Investigation Command (CCIC) and said he was aware of Adrian Lamo was in contact with an Army intelligence analyst releasing information to an Australian national [Julian Assange] in charge of Wikileaks

Chief of Staff to the President formerly Rahm Emmanuel

Chuck Hagel Co-Chair President's Intelligence Advisory Board

CIDNE (Combined Information Data Network Exchange) Afghanistan

CIDNE (Combined Information Data Network Exchange) Iraq

Citation United States v. Thomas Drake precluding harm on the merits

Classification and Assignment Board ("C&A Board")

Classification and Assignment Board ("C&A Board") which apparently met on a weekly basis to discuss PFC Manning's confinement conditions failed to properly document its recommendations on the required Bng Form 4200 for over five months

Classification determinations alone do not satisfy the mens rea requirement of 18 USC 793(e)

CLASSIFICATION REVIEW of the ten completed classification reviews provided six were four pages or less in length Of the remaining four classification reviews three were more than 12 pages in length and only one was over 30 pages in length

Classification spillage that the Government alleges occurred in March 2012 with the defense's original motions The Government said that the Defense had committed a spillage by inference namely that one could infer classified information Defense said at 23 Feb 2012 Arrangement that their experts determined there was "no spillage." Based upon...the Protective Order which defense filed the defense said that the Government unilaterally determines there is "spillage" Defense proposed at the 23 Feb 2012 Arrangement that the Court Security Officer have the ultimate authority in determining if there is a classification spillage and that the Court Security Officer consult the OCA's himself Later on defense remarked that although not in his email CPT Farn represented to him that the OCA recalled the latest incident constituted spillage Coombs asked CPT Farn to provide copies of any emails to the Defense and the Court that he sent to the OCA and received from the OCA regarding this issue. Farn did not indicate that he would provide the correspondence or any portion thereof

classified Microsoft PowerPoint Presentation on the original 5 July 2010 change sheet is alleged to have been obtained on SIPRNet which only contains information classified up to SECRET

Clause 1 of Article 134 offenses involve disorders and neglects to the prejudice of good order and discipline in the armed forces

Clause 2 of Article 134 offenses involve conduct of a nature to bring discredit upon the armed forces

Clause 3 offenses involve noncapital crimes or offenses which violate Federal law including law made applicable through the Federal Assimilative Crimes Act see subsection (4) below. If any conduct of the nature is specifically made punishable by another article of the code it must be charged as a violation of that article

Closed Session with "relevant Government agencies"

Closed session with "relevant Government agencies" and Special Agent David Shaver

Coast Guard Intelligence

COL Ricky Malone Quantico Brig Forensic Psychiatrist

Col. Carl R. Coffman Jr. Commander of Joint Base Myer and the Special Court Martial Convening Authority

Col. Carl R. Coffman Jr. Commander of Joint Base Myer and the Special Court Martial Convening Authority denied the defense's request to conduct oral depositions of nine essential witnesses including former Secretary of Defense Robert Gates and current Secretary of State Hillary Clinton Coffman determined that the "difficultly expense and/or effect on military operations outweighed the significance of the expected testimony" despite the possibility of the death penalty for Manning These same witnesses were requested by the defense for Manning's Article 32 Pretrial Hearing and were denied by Lt. Col. Paul Almanza a civilian career prosecutor at the Department of Justice. Almanza deemed that the "significance [of their testimony] does not outweigh military and governmental operations" and the witnesses were "not reasonably available given the importance of their respective position

Col. Daniel J. Cholea Quantico Base Commander

Col. David M. Miller Commander of the Second Brigade Combat Team (2BCT) 10th Mountain Division (10 MTN)

Col. David M. Miller Commander of the Second Brigade Combat Team (2BCT) 10th Mountain Division (10 MTN) said in a sworn statement for the Secretary of the Army's 15-6 investigation into unauthorized disclosure that commanders (in conjunction with their unit security manager) are allotted 30 days to submit an initial DA 5248-R following the discovery of credible derogatory information on a Soldier. After the initial DEROG is submitted and processed by SID/CFC (Security Investigations Division/ Central Clearance Facility) the unit has 90 days to submit a follow-up 5248-R if there is a pending investigation or adverse action taken (e.g. summary court-martial). Once the investigation/proceedings are completed and the Soldier has been cleared/charged of offense the unit must submit a final DEROG

Col. David M. Miller Commander of the Second Brigade Combat Team 10th Mountain Division also said Master Sergeant Paul David Adkins (now Sergeant First Class due to administrative action) "the NCIC Non Commissioned Officer in Charge) in the S2 Section and Pfc. Manning's commanding officer in the T-SCIF was marginal but not bad enough to either relieve or replace." According to the defense's account of Col. David M. Miller's sworn statement in the Secretary of the Army's 15-6 investigation into alleged unauthorized disclosure Col. David Miller said that Master Sergeant Paul David Adkins (now Sergeant First Class due to administrative action) "failed to inform the chain of command of Pfc. Manning emotional and mental condition and this failure resulted in the command not submitting a DEROG in a timely manner."

Col. David M. Miller sworn statement than Commander of the 10th Mountain Division's Second Brigade Captain Matthew W. Freiburg also relieved [A YET UNIDENTIFIED CAPTAIN] as the company commander for Headquarters and Headquarters Company 2nd Brigade 10th Mountain Division at the latter end of the 2BCT 10 MTN Div. deployment around April or May 2010 - a month or so before Pfc. Manning was arrested at FOB Hammer lag. According to the sworn statement of Col. David M. Miller the former company commander of HHC/2BCT 10 MTN Div. was relieved because "property accountability and due to the fact he was not making good decisions."

Col. David M. Miller's sworn statement "the officer in charge of PFC Manning" in the S2 Section of the 2nd Brigade 10th Mountain Division Maj. Cliff Clausen the Defense S2 "was not up to the standard of performance that [Col. David M. Miller] expected out of someone in that position." According to the defense's account of Col. David M. Miller's sworn statement Col. David M. Miller "decided it was best to remove" Maj. Cliff Clausen from his position as the [Brigade] S2 and place Captain Steven Lim into that job. According to the sworn testimony of Captain Steven Lim at the Article 32 Pretrial Hearing in the third or fourth week of January 2010 Captain Lim then the Assistant Brigade S2 was promoted to Brigade S2 replacing Maj. Cliff Clausen. Captain Lim testified that Maj. Cliff Clausen "could not communicate information to the commander [Col. David M. Miller] in the way the commander needed." Following a transition period on 6 February 2010 the command change in the S2 Section of the 2nd Brigade Combat Team 10th Mountain Division was official. Captain Steven Lim testified that the change in command was atypical because command rarely changes during deployment.

Col. Denise R. Lind is military judge for US v. Pfc. Manning

Col. Ricky Malone Quantico Brig Forensic Psychiatrist

Col. Robert G. Olman former former Security Battalion Commander

Col. Robert G. Olman former former Security Battalion Commander who said "I will not have anything happen to Manning on my watch... So nothing is going to change... He won't be able to hurt himself and he won't be able to get away and our way of making sure of that is that he will remain on Maximum Custody and PO indefinitely" and "We will do whatever we want to do. You make a recommendation and then I have to make a decision based upon everything else" and "Well that is what we are going to do"

Col. Stephen R. Henley asked Lt. Col. Paul Almanza if he was available to be Investigating Officer at US v. Pfc. Manning Article 32

Colonel Carl R. Coffman Jr. Commander of Joint Base Myer and the Special Court Martial Convening Authority

Command Judge Advocate at Quantico who was present in the January 13 2011 secret high level meeting about PFC Manning's confinement status

Common Law of War

Company Commander Drewser (sp.)

Company Commander Drewser (sp.) who Sergeant (former Specialist) Daniel Padgett testified that he did not talk to concerning the alleged December 2009 incident with Pfc. Manning

Computer Fraud and Abuse Act (CFAA)

Computer in Bradley Manning's aunt Debra Van Aalst's house powered on while he was in Iraq unnamed two (2) Army Computer Crimes Investigation Command (CCU) agents who went to the Department of State (State Department) (DOS) to collect cables

Cooler a soldier who worked on the night-shift with Sergeant (former Specialist) Daniel Padgett and Pfc. Manning under Captain Barclay Keay the first three weeks of Captain Barclay Keay's

deployment at FOB Hammer

Coombs: Number two...every one of the Government's witnesses was granted. In their request they listed just the names and no basis yet you granted all the witnesses they requested. Defense had 19 pages of relevance for each of the 38 names it requested 10 were government witnesses and they were granted. Of the 38 only two witnesses for the defense were granted. Then this morning two more were approved to the detriment of the defense to prepare in a case that involves death penalty [That means that 14 defense witnesses were granted]

Coombs: Under R.C.M. 902(a) the defense asks that you recuse yourself. R.C.M. 902(a)...just the mere existence of bias as follows: Number one...your position as a prosecutor for the DOJ a "career prosecutor" since 2002 coupled with an ongoing criminal grand jury...they would get a plea to go after Julian Assange. DOJ has not ruled out fact they would not rule out taking this case...you deny...but listening to the facts you are not impartial

Court Reporter

Court Reporter Cory Brothier (sp.)

Court Security Officer

Court's denial of the Defense Motion to Dismiss Specifications 13 and 14 of Charge II based on in this case

CW2 Denise Barnes (Former Quantico Base Commander) and one unknown individual whose name was redacted refused to change the decision to require PFC Manning to surrender his clothing and wear a smock at night after the 13 March 2011 incident

CW2 Denise Barnes decided to require PFC Manning to wear a suicide prevention article of clothing called a "smock" at night

CW2 Denise Barnes Former Quantico Bng Commander

CW2 Hondo Hack Brigade Fire Section

CW4 Airmen (sp.) Brigade S2 Section

CW4 James Averhart Former Quantico Brig Commander

CW4 James Averhart former Quantico Brig Commander stopped me and said "I am the commander" and that "no one could tell him what to do" He also said that he was for all practical purposes "God"

CW5 Abel Galaviz

CW5 Abel Galaviz's investigation of the conditions of PFC's Manning's confinement he found that the failure to immediately take PFC Manning off of Suicide Risk status upon the psychiatrist's recommendation was in violation of Navy rules"

CYBERCOM

DA 5248-R

Daniel Melzer President's Intelligence Advisory Board

Danny Clark

Danrell Edward Issa U.S. Representative for California's 49th congressional district Chair of the House Committee on Oversight and Government Reform

David Boren Co-Chair President's Intelligence Advisory Board

David Coombs lead civilian defense counsel to Major Ashden Fenn lead military prosecutor The Grand Jury investigation started in December of 2010 At that time the Defense requested access to the investigation being conducted by the DOJ

David Coombs lead civilian defense US v Pfc. Manning

David Coombs lead civilian defense US v Pfc. Manning "The Government has overcharged to strong-arm a plea from my client"

David Coombs lead civilian defense US v Pfc. Manning "We have had a breakdown from Major Clausen S2 all the way down to the most junior officer"

DCGS-A (Distributed Common Ground Systems)

DD Form 457

Dean Boyde Department of Justice spokesman (DoJ)

Debra Van Alstyne Bradley Manning's aunt

Defense discovery requests included FOIA for 2007 Apache Airstrike (Collateral Murder)

Defense discusses the Chain of Custody and Control for discovery as it relates to an Interagency investigation

Defense Information Systems Agency (DISA)

Defense Intelligence Agency (DIA)

Defense Intelligence Agency (DIA) An intelligence agency within the Department of Defense (DOD) which operated the Information Review Task Force (IRTF) a DOD (Department of Defense) directed organization that was responsible for conducting a comprehensive DOD (Department of Defense) review of classified documents posted to the Wikileaks website and any other associated materials

Defense Intelligence Agency (DIA) Final Security Violation Investigation Report

Defense Intelligence Agency (DIA) Information Review Task Force (IRTF) damage assessment

Defense motioned to close portions of the pretrial for an unnamed reason Coombs: "Defense has argued harm would come to client if certain details were made public"

Defense questions for ex parte motions

Defense requested that the Government provide among other things the classification determinations by the Original Classification Authorities (OCA) as well as the OCAs' damage assessments. This information was required to be completed by DOD Directive 5200.1 DOD Instruction 5240.4

Defense Secretary Robert Gates wrote a letter to Senator Carl Levin Chair of the Armed Services Committee citing findings by the Defense Intelligence Agency's (DIA) Information Review Task Force (IRTF): "The review to date has not revealed any sensitive intelligence sources and methods compromised by this disclosure." At the 18 October 2012 Article 39(a) Session Judge Lind ruled that the Court would take Judicial Notice of Defense Secretary Gates' letter to Senator Levin - for use in during sentencing since actual harm or damage is precluded from the merits without the Court's permission - citing Rule 801(c)(2)(d). The statement is not hearsay was given by a party opponent of the accused in United States v. Pfc. Bradley Manning and the statement "is one the party manifested that it adopted or believed to be true."

Department of Agriculture

Department of Defense (DoD)

Department of Defense (DoD) Damage Assessment of Compromised Information

Department of Energy's Office of Intelligence and Counterintelligence

Department of Homeland Security (DHS)

Department of Homeland Security (DHS) damage assessment

Department of Homeland Security Office of Intelligence and Analysis

Department of Homeland Security Office of Intelligence and Analysis (DHS/OIA)

Department of Housing and Urban Development

Department of Justice (DoJ)

Department of Justice (DoJ) The Government collaborated with the federal prosecutors within the DOJ (Department of Justice) during the accused's (Manning) investigation

Department of State (State Department) (DoS)

Department of State (State Department) (DoS) 24/7 WikiLeaks Working Group

Department of State (State Department) (DoS) briefing of House and Senate on December 2 2010

Department of State (State Department) (DoS) briefing of House Permanent Select Committee on Intelligence (HPSCI) on December 7 and 9 2010

Department of State (State Department) (DoS) briefings to Congress

Department of State (State Department) (DoS) Cables (cablegate)

Department of State (State Department) (DoS) Chiefs of Mission Review

Department of State (State Department) (DoS) Circle Log Files

Department of State (State Department) (DoS) damage assessment

Department of State (State Department) (DoS) did not embark on an effort update its damage assessment after the entire diplomatic database was released in unredacted form in September of 2011

Department of State (State Department) (DoS) Executive Secretariat Ambassador Stephen D. Mull

Department of State (State Department) (DoS) Firewall Logs

Department of State (State Department) (DoS) Firewall Logs for the IP addresses 22.225.41.22 and 22.225.41.40 associated with the Dell 40 and Alienware 22 machines respectively. Show amount of connections

Department of State (State Department) (DoS) forensic results

Department of State (State Department) (DoS) investigative file

Department of State (State Department) (DoS) Operations Center

Department of State (State Department) (DoS) The accused (Manning) is charged with compromising the DoS's documents and the Government intends to use additional information from the Department during its case-in-chief

Department of State (State Department) (DoS) Web Server Logs

Department of State (State Department) (DoS) Web Server Logs for the IP addresses 22.225.41.22 and 22.225.41.40 associated with the Dell 40 and Alienware 22 machines respectively. Shows amount of connections

Department of State (State Department) (DoS) WikiLeaks Mitigation Team

Department of State (State Department) (DoS) WikiLeaks Mitigation Team The list of meeting dates/times [of the WikiLeaks Mitigation Team and the Department of State (State Department) (DoS) is inconsistent with the testimony of Department of State (State Department) (DoS) witnesses who believed that these meetings ended sometime in the summer of 2011. In reality the Mitigation Team was still meeting as of 19 December 2011

Department of State (State Department) (DoS) WikiLeaks Persons at Risk Working Group

Department of the Army Inspector General (DAIG)

Department of the Treasury Office of Intelligence and Analysis

Despite a bill of particulars request covering the Government's theories underlying the 18 USC Section 641 specifications the Government refused to articulate its theory of how PFC Manning stole or knowingly converted Government databases that remained in the possession of the United States. While at the time the Defense believed the Government was just engaging in some improper gamesmanship the Defense now believes in light of the Government's confusion over its own "exceeds authorized access" theory (or theories) that the Government simply did not yet have an articulable legal theory for the theft or knowing conversion specifications

Despite Capt. Hocter forensic psychiatrist for the Quantico brig and COL Malone's forensic psychiatrist for the Quantico brig consistent recommendations I remained on POI watch and in MAX custody

DIACAP (Department of Defense Information Assurance Certification and Accreditation Process)

Diplomatic Security Service (DSS) The primary law enforcement organization within the Department of State (State Department) (DoS) focused on investigating matters related to the ODS

Diplomatic Security (DSS) Agent who interviewed Bradley Manning's aunt Debra Van Aalstye

Diplomatic Security Service (DSS) The Government has turned over limited files from joint investigation with DSS. The discovery provided deals only with the item charged in Specification 14 of Charge II. The Government has not turned over any DSS files or investigation dealing with Specifications 12 or 13 of Charge II

Diplomatic Security Services (DSS) at the Department of State (State Department) (DoS)

Disc utility log for Manning's MacBook Pro that had entries between February 27 2010 and March 9 2010

DOD Directive 5200.1

DOD Directive 5210.50

DOD Instruction 5240.4

DOJ (Department of Justice) The Government collaborated with the federal prosecutors within the DOJ during the accused's investigation

Drug Enforcement Administration Office of National Security Intelligence (ONSI)

DS Channel (for messages between the Assistant Secretary and/or Deputy Assistant Secretaries of Diplomatic Security other authorized DS personnel and the responsible DS officer concerning criminal and special investigations involving US citizens US Government employees or DS employees counterintelligence investigations adverse personnel security actions; investigations concerning domestic abuse; confidential sources undercover operations and other sensitive subjects which the drafter deems should be highly restricted. Limit field dissemination of DSX CHANNEL messages to the regional security officer or post security officer limit domestic dissemination to specific offices within DS. The Director of the Office of Investigations and Counterintelligence (DS/OSSI/OCI) authorizes access to DSX Channel message traffic at the headquarters level. See US Department of State (State Department) (DoS) Foreign Affairs Manual Volume 5 Handbook 2 Telecommunications Handbook for more info)

DS-controlled (DSX CHANNEL)—for messages between the Assistant Secretary and/or Deputy Assistant Secretaries of Diplomatic Security other authorized DS personnel and the responsible DS officer concerning criminal and special investigations involving US citizens US Government employees or DS employees counterintelligence investigations adverse personnel security actions; investigations concerning domestic abuse; confidential sources undercover operations and other sensitive subjects which the drafter deems should be highly restricted. Limit field dissemination of DSX CHANNEL messages to the regional security officer or post security officer limit domestic dissemination to specific offices within DS. The Director of the Office of Investigations and Counterintelligence (DS/OSSI/OCI) authorizes access to DSX Channel message traffic at the headquarters level. See US Department of State (State Department) (DoS) Foreign Affairs Manual Volume 5 Handbook 2 Telecommunications Handbook for more info)

Duty Brig Supervisor ("DSB")

Dynadot

either way there is a period of unexplained delay & that delay was caused by some arm of the United States Govt

Element no. 1 of an Article 52 (1) offense for a violation of AR 380-5 There was in effect a certain lawful general order or regulation in the following terms: Paragraphs 1-21 and 6-1 Army Regulation 380-5 dated 29 September 2000

Element no. 2 of an Article 52 (1) offense for a violation of AR 380-5 (2) The accused had a duty to obey this regulation and

Element no. 3 of an Article 52 (1) offense for a violation of AR 380-5 (3) That on diverse occasions between on or about [varying date ranges] and/or near Contingency Operating Station Hammer Iraq the accused violated this lawful general regulation by knowingly willfully or negligently disclosing classified or sensitive information to unauthorized persons

Element of Clause 1 of Specification 1 of Charge II charges Under Article 134 (1) The accused at or near Contingency Operating Station Hammer Iraq between on or about 1 November 2009 and on or about 27 May 2010 wrongfully and wantonly caused to be published on the internet intelligence belonging to the United States having knowledge that intelligence published on the internet is accessible to the enemy and

Element of Clause 2 of Specification 1 of Charge II charges Under Article 134 (2) Under the circumstances the conduct of the accused was to the prejudice of good order and discipline in the armed forces and of a nature to bring discredit upon the armed forces

Elements no. 1 of charges under 18 USC 793(e) violations charged in Specifications 2 3 5 7 9 10 11 and 15 of Charge II (1) The accused at or near Contingency Operating Station Hammer Iraq between on or about [varying date ranges] had unauthorized possession of information

Elements no. 2 of charges under 18 USC 793(e) violations charged in Specifications 2 3 5 7 9 10 11 and 15 of Charge II (2) The information was relating to the national defense to wit [the named information]

Elements no. 3 of charges under 18 USC 793(e) violations charged in Specifications 2 3 5 7 9 10 11 and 15 of Charge II (3) The accused knew or had reason to believe that the information could be used to the injury of the United States or to the advantage of any foreign nation

Elements no. 4 of charges under 18 USC 793(e) violations charged in Specifications 2 3 5 7 9 10 11 and 15 of Charge II (4) The accused willfully communicated delivered or transmitted or caused to be communicated delivered or transmitted the information to a person not entitled to receive it and

Elements no. 5 of charges under 18 USC 793(e) violations charged in Specifications 2 3 5 7 9 10 11 and 15 of Charge II (5) Under the circumstances the conduct of the accused was to the prejudice of good order and discipline in the armed forces and of a nature to bring discredit upon the armed forces

Ellen Lajpsov President's Intelligence Advisory Board

Email correspondence between then-CPT Pen and the Brig officials demonstrates that the Government was not at all concerned with seeing PFC Manning's confinement conditions reconsidered but was instead solely concerned with combating a potential Article 13 Motion

Email Reel Bradley Manning sent to Master Sergeant Paul David Atkins (now Sergeant 1st Class due to administrative action) with a photo of himself dressed as a woman

Encase forensic image of each computer from the T-SCIF or seized by the Government

Enemy: Entity specified in Bates Number 00410660 through 00410664

Environmental Protection Agency (EPA)

Eric Schmied

Eric Stein the transcriber of the WikiLeaks Mitigation Team at the Department of State (State Department) (DoS)

Every court interpreting Article 104(2) must prove general criminal intent to give intelligence to or communicate with the enemy indeed no prosecution under this Article has ever been maintained without some allegation of mens rea

EXDIS (For messages needing exclusive distribution to officers with essential need to know. Use this caption only for highly sensitive traffic between the White House the Secretary Deputy or Under Secretaries of State and chiefs of mission see 5 FAH-2 H-442.6 When and How to Use EXDIS See US Department of State (State Department) (DoS) Foreign Affairs Manual Volume 5 Handbook 2 Telecommunications Handbook for more info)

Executive Office of Management and Budget (OMB)

Farah.zip [Defense mentions this on cross-examination in relation to three videos but it is unclear]

Federal Bureau of Investigation (FBI)

Federal Bureau of Investigation (FBI) Diplomatic Security Services (DSS) at the Department of State Department of State (State Department) (DoS) Department of Justice (DoJ) Government Agency Office of the Director of National Intelligence (ODNI) Office of the National Counterintelligence Executive (ONCE) and files in relation to PFC Manning and/or Wikileaks

Federal Bureau of Investigation (FBI) forensic results

Federal Bureau of Investigation (FBI) impact statement

Federal Bureau of Investigation (FBI) investigative file

Federal Bureau of Investigation (FBI) participated in a joint investigation of the accused and even though the Government has ready access to this material

Federal Bureau of Investigation (FBI) The primary law enforcement organization within the DoJ (Department of Justice) focused on investigating matters related to the accused (Manning)

Federal Communications Commission (FCC)

Federal Rule 16

Federal Trade Commission (FTC)

Files linked to the fraudulent station in the database [Unclear from Reiman or the transcriber's notes what this refers where it was found or what it refers to]

files.zip

First instance of WGEI in March 2010 that Special Agent David Shaver Computer Crimes Investigation Command (CCIU) asserts seemed to be to access the Gitmo detainee assessments. [Transcriber notes the date may have been 7 March 2010 but it is not clear which computer and where this was found] Special Agent David Shaver Computer Crimes Investigation Command (CCIU) said an unnamed forensic examiner was able to recreate the script and download Gitmo detainee logs on his own computer. The forensic unit then downloaded the Gitmo logs published by WikiLeaks and compared them to what they pulled via the WGEI script. According to Special Agent David Shaver Computer Crimes Investigation Command (CCIU) they matched

First Lieutenant Elizabeth Fields Special Security Representative (SSR) for the T-SCIF 52 Section 2nd Brigade Combat Team (2 BCT) 10th Mountain Division (10 MTN Div.)

Five unnamed people who Special Agent Toni Graham Army CID interviewed faced to face (one of them was Captain Casey Martin (named name Fulton) Platoon leader and Brigade Assistant 52 Officer concerning Collateral Murder) and other unnamed people she canvassed who knew Manning

Flight Into Hypermasculinity

FOIA Requests Regarding Video in Specification 2 of Charge II (Collateral Murder) (12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone av.)

For any captioned or otherwise particularly sensitive documents (as explained below to include NODIS [The use of the NODIS caption identifies messages of the highest sensitivity between the President the Secretary of State and chief of mission. You must not distribute NODIS messages to anyone other than the intended recipient without prior approval from the Executive Secretariat (SES-O). See US Department of State (State Department) (DoS) Foreign Affairs Manual Volume 5 Handbook 2 Telecommunications Handbook for more info] EXDIS [For messages needing exclusive distribution to officers with essential need to know. Use this caption only for highly sensitive traffic between the White House the Secretary Deputy or Under Secretaries of State and chiefs of mission; see 5 FAH-2 H-442.6 When and How to Use EXDIS See US Department of State (State Department) (DoS) Foreign Affairs Manual Volume 5 Handbook 2 Telecommunications Handbook for more info] ROGERS CHANNEL [for communications between the Assistant Secretary for Intelligence and Research (NIR) and the chief of mission See US Department of State (State Department) (DoS) Foreign Affairs Manual Volume 5 Handbook 2 Telecommunications Handbook for more info] DS Channel [for messages between the Assistant Secretary and/or Deputy Assistant Secretaries of Diplomatic Security other authorized DS personnel and the responsible DS officer concerning criminal and special investigations involving US citizens or foreign nationals who are not US Government employees, special protective equipment; and other sensitive subjects which the drafter deems should be restricted to DS personnel at posts or within the Department. See US Department of State (State Department) (DoS) Foreign Affairs Manual Volume 5 Handbook 2 Telecommunications Handbook for more info] or DS-controlled [DSX CHANNEL--for messages between the Assistant Secretary and/or Deputy Assistant Secretaries of Diplomatic Security other authorized DS personnel and the responsible DS

officer concerning criminal and special investigations involving U.S. citizens US Government employees or DS employees; counterintelligence investigations, adverse personnel security actions, investigations concerning domestic abuse; confidential sources; undercover operations; and other sensitive subjects which the drafter deems should be highly restricted. Limit field dissemination of DSX CHANNEL messages to the regional security officer or post security officer; limit domestic dissemination to specific offices within DS. The Director of the Office of Investigations and Communications (DS/DOS/IC) authorizes access to DSX Channel message traffic at the headquarters level. See US Department of State (State Department) (DoS) Foreign Affairs Manual Volume 5 Handbook 2 Telecommunications Handbook (for more info) for which redactions are not sought the Department will make the documents available to the defense counsel fan their security experts to inspect at the Department until the end of the Court-martial. For all remaining documents for which redactions are not sought the prosecution will deliver these documents to the defense by 21 September 2012. The defense counsel and their experts are not authorized to share the information contained within these documents of their notes with the accused

For over a year the Government justified its need for excludable delay to the Convening Authority in part due to the requirement to obtain these Original Classification Authority (OCA) classification determinations. The Government provided these determinations to the Defense piecemeal. It was not until the late fall (approximately November 2011) that the Defense had in its possession all of the OCA classification determinations

Forensic evidence unequivocally established that PFC Manning did not use Wiget to obtain the information in Specification 14 of Charge II

forensic imaging of the WikiLeaks website by CCUI

FORSOM

Fort Huachuca

Four Quantum Guards

Four T-SCIF computers that the Government represented would be produced on 18 May 2012 On 16 April the Government stated it was confident that the 4 computer hard drives could be provided by 18 May 2012 The computer hard drives were not provided on 18 May 2012 On 29 May the Defense asked when it should expect to receive the hard drives The Government indicated that they would have approval by the end of the week As of 2 June 2012 the Government still has not produced these four hard drives

Full investigative files by U.S. Army Criminal Investigation Command (CID) Defense Intelligence Agency (DIA) Defense Information Systems Agency (DISA) CENTCOM SOUTHCOM related to PFC Manning

Further a congressional aid who spoke to Reuters and who was also "familiar with the late 2010 briefings" by the State Department said "We were told (the impact of WikiLeaks revelations) was embarrassing but not damaging"

Games

Garani Air Strike Video

General Court Martial Convening Authority (GCMCA)

General James Jones the President's former National Security Advisor

George W. [last name sounds like "Street"] Reitman notes the name as George W. Shriek (sp.) WHO IS THIS? FBI? provided with alleged chat logs between Adrian Lamo and bradass87 on two thumb drives BY WHOM?

George W. [last name sounds like "Street"] WHO IS THIS? FBI? provided with alleged chat logs between Adrian Lamo and bradass87 on two thumb drives BY WHOM?

GEOTRANS an application program which allows a user to easily convert geographic coordinates among a wide variety of coordinate systems map projections and datums

Given the fact the OCA determinations are merely probative on the element of the 18 USC 793(e) offense the Defense should be entitled to examine the basis for the OCA determinations as to why the information was classified and the OCA's belief regarding whether the reviewed information really "could" cause damage to national security

Google

Google Earth

Google search records for a Bradley Manning user profile on a NIPRNet computer that included a profile for Bradley Manning

Government also presented chats alleging Nathaniel Frank who the Government alleges is Julian Assange offered assistance to Manning in cracking a logon password to allow him to search anonymously on a computer

Government argues that the authorization for installing mIRC and the like [the examples of unauthorized programs installed on computer] came from the Chain of Command and not technical restrictions [need for admin privileges for example]

Government cannot assert that this case is overly complex or that it raises novel issues while simultaneously turning a blind eye to the fact that a substantial portion of that complexity and novelty has been caused by the Government's own charging decision In other words the Government cannot be given a free pass on the reasonable diligence inquiry simply by asserting the complexity of the case especially when it has charged the case in such a complex manner that necessitated delay in the proceedings to allow the Government to mull over how it can make the proof fit its lofty and imaginative charging decision

Government Ex Parte RCM 701(g)(2) Motion for a Department of Homeland Security (DHS) document. The motion and its enclosures are being submitted via NIPR in a separate email. Attached to this email is a redacted version for the defense

Government MRE 505(g)(2) Motion for Central Intelligence Agency (CIA) (Government Agency) Information. The motion and its enclosures are being submitted via SIPR and hand delivery on Monday

Government MRE 505(g)(2) Motion for DOS Information. The motion and its enclosures are being submitted via NIPR in this email. Two of the enclosures are being submitted via NIPR in a separate email

Government Notice to the Court for Government MRE 505(g)(2) Motion for Department of State (State Department) (DoS) and Central Intelligence Agency (CIA) (Government Agency) Information which includes the unclassified and redacted version of the Central Intelligence Agency (CIA) (Government Agency) motion

Government Notice to the Court for Office of the Director of National Intelligence (ODNI) Information

Government placed PFC Manning in administrative hold with escorts on 27 May 2010 and placed PFC Manning in pretrial confinement on 29 May 2010

Government responded to all of the Defense request of a Bill of Particular except three items

Government Supplemental Filing for MRE 505(g)(2) Filing for FBI Investigative File. The supplement is attached. The classified enclosures are being submitted ex parte via SIPR and hand delivery on Monday

Government wanted to delay the trial until 18 May 2012 to decide whether to assert a privilege with respect to any classified information

Government was advice that it must provide a Bill of Particulars Government did with the exception of three

Government's interest in securing a conviction and making an example out of PFC Manning has clouded the prosecutors' professional judgment This is apt to happen in high-profile cases It is no coincidence that many high-profile cases are plagued by serious discovery violations

Government's lack of diligence in this case independent of the discovery issues. Among them: The Government has repeatedly requested additional time to complete simple tasks and to respond to straightforward motions The Government has repeatedly promised to "get back to" the Court on various issues in oral argument and rarely does The Government still has not provided "timely and meaningful" access to Ambassador Kennedy as promised when it returned the Defense to file a Touby request The Government has frequently shifted litigation positions suggesting that its positions are borne of convenience and not of principle (consider for instance the Government's three-shifting argument on whether Army Regulation 380-5 was punitive in nature and its arguments on "exceeds authorized access") The Government's email system has been plagued by errors that still have not been fixed. Given the volume of email traffic these issues should have been sorted out months ago The Government's about-face on complying with the Protective Order with respect to Defense redacted motions. The Government argued that it was simply too difficult for it to continue reviewing the redactions The Government's failure to organize logistical issues in a timely manner (eg its requirement for a 30 day OPLAN Bravo Order prior to the Article 32 etc.)

Grand Jury Testimony or Files

graymailing

Gnd Extractor a binary executable capable of extracting MGRS grids from multiple free text documents and importing them into a Microsoft Excel spreadsheet

Guantanamo Detainee Profiles (GTMO files)

Guantanamo Detainee Profiles (GTMO files) are marked SECRET

Gunnery Sergeant Blenis at Quantico

H R. 553 The Reducing Over-Classification Act President Barack Obama 7 October 2010

Headquarters Battalion Commander "the first accuser" and convening authority

Headquarters Department of the Army (HQDA)

Headquarters Department of the Army (HQDA) 17 April 2012 memo

House Committee on Oversight and Government Reform

House Permanent Select Committee on Intelligence (HPSCI)

How many links in the chain of "indirectly" could render the soldier subject to the death penalty?

Howard Schmidt: a former Tiversa adviser is cybersecurity coordinator and special assistant to U.S. President Barack Obama

Human Health Services (HHS)

I asked the Brig Operations Officer MSG (Marines Security Guard) Papake what I needed to do in order to be downgraded from Maximum Custody and POI Status MSG (Marines Security Guard) Papake Brig Operations Officer responded by telling me that there was nothing I could do to downgrade my detainee status and that the Brig simply considered me a risk of self-harm

I walked towards the front of my cell with my hands covering my genitals The guard told me to stand a parade rest which required me to stand with my hands behind my back and my legs spaced shoulder width apart I stood at "parade rest" for about three minutes until the OBS (Duty Brig Supervisor ("DBS") arrived

I was approached by GYSGT (Gunnery Sergeant) Blenis He asked me what I had done wrong I told him that I did not know what he was talking about He said that I would be stripped naked at night due to something that I had said to Brig Operations Officer MSG (Marines Security Guard) Papake

Iceland

Images of the raw structure of files in the Farah investigation folder on the CENTCOM servers related found from a specific path to that folder found in the index.dat on the Alienware .22. Shaver said the file structure matched found in the index.dat matched the CENTCOM server

Immigration and Customs Enforcement (ICE)

In addition to going toward a key element of three separate offenses the Defense maintains that the absence of damage is relevant for the impeachment of Government witnesses who claim that the leaks could cause damage The Government however believes that the use of a damage assessment to impeach an Original Classification Authority (OCA) who prepared a classification review would be improper

In an email to Master Sergeant (now Sergeant 1st class due to an administrative action) Adkins Pfc. Manning wrote: "This is my problem. I've had signs of it for a very long time. I've been trying very hard to get rid of it. I thought military would get rid of it. But it is not going away. It is haunting me more and more as I get older. Now the consequences are getting harder. I am not sure what to do with it. It is destroying my ties with family. It is preventing me from developing as a person. It is the cause of my pain and confusion. It makes the most basic things in my life very difficult. The only solution is getting rid of me. The fear of getting caught has made me cover up. It is difficult to sleep and impossible to have conversations. It makes my entire life feel like a bad dream that won't end. I don't know what to do. I don't know what to do. I don't know what will happen to me. But at this point I feel like I am not here anymore. Everyone is concerned about me and everyone is afraid of me. I am sorry." - Pfc. Bradley Manning

In mid-June 2012 the Government notified the Defense that it had "discovered" an Federal Bureau of Investigation (FBI) impact statement

In Re Application of the USA For an Order Pursuant to 18 USC § 2703(d) for Twitter

In the allocated space on the Alienware .22 computer Wget was found to be added on 4 May 2010 but Special Agent David Shaver Computer Crimes Investigation Command (CCU) testified that he found an earlier version in Windows Prefetch folder

In the allocated spaces on the Alienware .22 computer under Bradley Manning's user profile

In the unallocated spaces of the Alienware .22 "thousands" of complete cables ranging in classification and "many" incomplete ones

In total from the commencement of PFC Manning's pretrial confinement until PFC Manning's arraignment on 23 February 2012 there were 323 days in which no apparent Government activity has occurred

incident at Fort Drum in May 2009 between Specialist Jihraah Showman and Bradley Manning

Incident with Pfc. Manning curled in the fetal position on the floor the night Pfc. Manning allegedly struck Specialist Jihraah Showman

Incident with Sergeant (former Specialist) Daniel Padgett December 2009

Incident with Specialist Jihraah Showman May 7 2010

Incident with the Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) and a projector in December 2009 or January 2010

Information Review Task Force (IRTF)

Intelink

Intelink Log Files

Intelink Logs Forensic Report (Classified Attachment)

Intelink logs from October 2009 to May 2010

Intelink search queries associated with the IP address 22.225.41.22 between 9 January 2010 and 21 April 2010

Intelink search queries associated with the IP address 22.225.41.40 between 1 December 2009 and 08 March 2010. Special Agent David Shaver Computer Crimes Investigation Command (CCU) asserts these contain search queries for WikiLeaks Julian Assange and Iceland (transcriber also noted the search term "wikileaks"). Special Agent David Shaver Computer Crimes Investigation Command (CCU) asserts there were 100 searches conducted for the term WikiLeaks

Intelink search queries eight (8) searches for information related to "retention of interrogation video". These were associated with the IP address 22.225.41.40 between 28 November 09 and 17 January 2010

Intelligence Community (IC)

Interagency Committee Review

Iraq War Diary

It was determined that for search warrants and special warrants needed from a Federal judge. Special Agent Mark Mander Army Computer Crime Investigative Unit (CCU) mentions Google and Twitter console leads and the technical nature of the matter more suited to Army Computer Crime Investigative Unit (CCU)

It was the government's decision to conduct this Article 32 investigation at Fort Meade

Jacob Appelbaum

Jacob Appelbaum Google

Jacob Appelbaum Sonic

Jacob Appelbaum Twitter

Jacob Law former Director of the Executive Office of Management and Budget (OMB)

Jacob Law former Director of the Executive Office of Management and Budget (OMB) 28 November 2010 "WikiLeaks Mishandling of Classified Information"

James Clapper Director of the Office of National Intelligence (ODNI)

James Cully 4th Cavalry Division Brigade S2 is the Official Classification Authority for classification review of the unclassified July 12 2007 Baghdad airstrike videos also known as "Collateral Murder"

Jason Allen Millman a field software engineer contractor's civilian boss

Jason Allen Millman was a field software engineer contractor at F.O.B. Hammer Iraq. His jobs was to keep the DCGS-A up and running

Jason Allen Millman was the only one in the T-SCIF with administrator privileges

Jason Katz

Joint Readiness Training Center (JRTC)

Joint Regional Correctional Facility Fort Leavenworth Kansas

JTF-GTMO

Juan Mendez UN Special Rapporteur on Torture

Judge Lind acknowledges that the order proposing that the Court Security Officer is [not signed]. [I have in my notes that this individual is "EB". I also have in my notes that the defense mentions the individual Prather (sp.) related to the Protective Order.]

Judge Lind cited the following case law in her ruling: Rule 401. Scope of probative evidence in military commissions Rule 403. Exclusion of probative evidence on grounds of prejudice confusion or waste of time Rule 410. Inadmissibility of plea discussions and related statements US v. White 606 F.3d 144 (4th Cir. 2010) concerning "a conviction for assault and battery in VA does not require physical force" as an element of the crime" Rules for Court-Martial 703(b) Right to witnesses. US v. Diaz concerning "the mens rea requirement of the Espionage Act "Willfulness" in the context of § 793(e) arises not in the context of bad intent but in the conscious choice to communicate covered information"

Judge Lind: This case deals with classified info. There are over three million pages of documentation in this case. Has the classified information been disclosed to Defense?

Joshua Mack President's Intelligence Advisory Board

Julian Assange

JWICS Joint Worldwide Intelligence Communications System)

Kay Gotoh took over for Marguerite Coffey former State Department director of the Office of Management Policy Right Sizing and Innovation who also acted as the supervisor of the WikiLeaks Mitigation Team prior to that she was Coffey's deputy

Kevin Poulsen

Kim Zetter

Lance who dealt mostly with HQ

Lee Hamilton President's Intelligence Advisory Board

Leon Panetta former director of the Central Intelligence Agency (CIA) current Secretary of Defense at the Department of Defense

Lester Lyles President's Intelligence Advisory Board

Linux work computer seized from Jason Katz at Brookhaven National Labs at the Department of Energy

List of 2703.d orders under seal for Docket No. 10GU379

Lt. Col. Brian Kems Executive Officer (XO) 2nd Brigade Combat Team 10th Mountain Division

Lt. Col. Brian Kems Executive Officer (XO) 2nd Brigade Combat Team 10th Mountain Division was Major Cliff Clausen's direct supervisor

Lt. Col. Cameron Leiker Headquarters Battalion Commander

Lt. Col. Dawn Hilton Commander Joint Regional Correctional Facility at Fort Leavenworth

Lt. Col. Eric Fleming Headquarters Command Battalion

Lt. Col. Mark Holzer was Lt. Col. Paul Almanza Article 32 Investigating Officer legal advisor

Lt. Col. Paul Almanza Article 32 Investigating Officer

Lt. Col. Paul Almanza Investigating Officer at the Article 32 Preliminary Hearing ruled on damage assessment and closely aligned organizations: Central Intelligence Agency (CIA) The "evidence is not reasonably available as this was a joint investigation this evidence is cumulative with evidence of the CID case file and its limited significance is not outweighed by the delay in obtaining this evidence"

Lt. Col. Paul Almanza Investigating Officer at the Article 32 Preliminary Hearing ruled: Quantico Video: The "evidence is not relevant to the form of the charges the truth of the charges or information as may be necessary to make an informed recommendation as to disposition specifically the circumstances surrounding PFC Manning's placement in suicide risk are not relevant to a determination as to whether PFC Manning committed the charged offenses and if so what the disposition of those charges should be"

Lt. Col. Paul Almanza's unnamed supervisor at the DoJ with whom he spoke to about the case Coombs: Discussed this information with anyone [referring to preliminary hearing]? ID... supervisor

Lt. Gaff (sp.)

Lt. General George J. Flynn, 3 Star General who ordered that Manning be held in MAX and in POI at Quantico Director Director J-7 Joint Staff

Lt. General Robert E. Schmidle Deputy Commander US CYBERCOM

Lt. General Robert L. Caslen

Lt. Hughs at Fort Meade MD guarding the proceedings of US v Pfc. Manning

Major Ashden Fein lead military prosecutor in US v Pfc. Manning

Major Ashden Fein lead military prosecutor in US v Pfc. Manning "Pfc. Manning knew that the enemies of the United States were using the Internet and that they could access WikiLeaks"

Major Ashden Fein lead military prosecutor in US v Pfc. Manning "Pfc. Manning used WikiLeaks' most wanted list" as a guiding light"

Major Ashden Fein lead military prosecutor in US v Pfc. Manning: "By searching for WikiLeaks Manning found info on how transmitting classified information to WikiLeaks could do harm. Known terrorist entities like Al Qaeda use WikiLeaks for their own information."

Major Ashden Fein lead military prosecutor in US v Pfc. Manning: "On 22 May 2010

Major Ashden Fein's letter to the General Counsel of the Office of the National Counter Intelligence Executive (ONCIX)

Major Cliff Clausen Brigade S2

Major Cliff Clausen sworn statement Major Clausen does not recall talking to the former YET UNIDENTIFIED CAPTAIN] and company commander of HHC/2BCT 10 MTN Div. about PFC Manning's behavioral health issues. According to the defense's account of the sworn statement of Col. David M. Miller that former [YET UNIDENTIFIED CAPTAIN] and company commander of HHC/2BCT 10 MTN Div. was relieved by Captain Matthew W. Freeburg in April or May of 2010 because of "properly accountability and due to the fact he was not making good decisions."

Major Cliff Clausen was the Brigade S2 2nd Brigade Combat Team 10th Mountain Division until January 2010 and provided a sworn statement for the Secretary of the Army's 15-6 investigation into the alleged unauthorized disclosures. Major Cliff Clausen was Pfc. Bradley Manning's most senior commanding officer in the Brigade S2 Section until January 2010.

Major Cliff Clausen who Captain Steven Lim 2nd Brigade Military Intelligence (MI) Company Commander Brigade S2 replaced when Major Cliff Clausen was removed because according to Captain Steven Lim 2nd Brigade Military Intelligence (MI) Company Commander Brigade S2 Major Cliff Clausen could not communicate information to the Commander in a way Commander needed

Major Gen. Michael S. Linnington Commander of Joint Task Force - National Capital Region the General Court Martial Convening Authority

Major Matthew Kemkes former military defense counsel for Pfc. Manning asserted at the Article 32 Pretrial hearing that SA Graham's Army CID 29 May 2010 affidavit was a "major piece of documentation" affecting Manning's pre-trial confinement hearing

Major Matthew Kemkes military defense US v Pfc. Manning

Major Thomas Hurley military defense US v Pfc. Manning

ManTech International

Manual for Military Commissions (MMC)

March 14 at 7:35pm Government says we notified civilian counsel that we dropped a CD with 12 Pages of discovery that refers to impeachment information that questions credibility of witness) on Adrian Lamo

March 2010 did you know about an equal employment complaint that according to Captain Steven Lim 2nd Brigade Military Intelligence (MI) Company Commander Brigade S2 involved intense threats

Marguerite Coffey former Department of State (State Department) (DoS) director of the Office of Management Policy Right Sizing and Innovation who also acted as the supervisor of the WikiLeaks Mitigation Team

Marguerite Coffey former State Department director of the Office of Management Policy Right Sizing and Innovation who also acted as the supervisor of the WikiLeaks Mitigation Team

Marine Corps Intelligence

Marine Security Guard Papakie at Quantico Brig Operations Officer

Mark Johnson ManTech International Contractor reports to Special Agent David Shaver Army Computer Crimes Investigative Unit (CCIU)

Mark Rasch

Master Sergeant Brian Paki (sp.)

Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action)

Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) wrote three memoranda Memorandum One: "Pfc. Manning's instability heightened in 2009." "Psychiatric care one to two times a week might have helped Manning. Yet Master Sergeant Adkins did nothing. Memorandum Two: "Pfc. Manning exhibits bizarre behavior... event's reemerged." "Adkins wrote that memo and yet did nothing. Memorandum Three: "Manning was sitting upright knees clutched as though in pain." Adkins noticed an open Gerber knife. "Manning had etched on his seat 'I want with the blade. He felt that he was not there, was not a person. He said he was a turtle with a core personality and several layers of hard shell to protect his personality. He seemed able to recover." Adkins wrote that memo and yet did nothing. That night Manning struck Showman

McGrath is also the Department of State's primary liaison to the National Counterterrorism Center where Russel Travers was Deputy Director in charge of the NCTC's "authoritative database supporting the Terrorist Screening Center and the USDO's watch listing system" before the President's National Security Advisor picked him to head the NSS' Interagency Committee Review of WikiLeaks. As it turns out McGrath is also the Department of State's primary liaison to Terrorist Screening Center (TSC) - an inter-agency organization lead by the FBI and responsible for a "single database of identifying factors" about individuals suspected by the UGS of involvement in terrorist activities. The TSC maintains the "Terrorist Watch-list" the "No-Fly List" as well as the "Selectee List" - the latter two being subsets of the Terrorist Screening Database (TSDb) used by the Transportation Security Administration - which associates and supporters of Julian Assange Bradley Manning and WikiLeaks have found themselves detained and interrogated by means of including: David House, Jacob Appelbaum, Jennifer Robinson and with her experience on the "inhibited list" and others.

Military Commissions Act

Military District of Washington (MDW)

Military Judges Bench Book

Millennium Challenge Corporation

mIRC

Model Specification

Mona Sutphen President's Intelligence Advisory Board

Motion for the Investigating Officer Lt. Col. Paul Almanza to Recuse himself

Movies

MP Bradley at the Security Officers desk during the Article 32 Pretrial Hearings of US v Pfc. Bradley Manning

Mr. Betts US Cyber Command Chief Classification Officer made a classification determination for "the alleged chat logs" and the information contained therein

Music

National Archives

National Counterterrorism Center (NCTC)

National Geospatial-Intelligence Agency

National Reconnaissance Office

National Security Agency (NSA)

National Security Council

National Security Council Insider Threat Task Force

National Security Staff (NSS) Steering committee

Neil MacBride U.S. Attorney for the Eastern District of Virginia

Net Centric Diplomacy Database

New York Times

NIPRNet computer from the Supply Room at FOB Hammer Iraq

NIPRNet computer that included a profile for Bradley Manning

NODIS (The use of the NODIS caption identifies messages of the highest sensitivity between the President the Secretary of State and chief of mission. You must not distribute NODIS messages to anyone other than the intended recipient without prior approval from the Executive Secretariat (S/E-S-O). See US Department of State (State Department) (DoS) Foreign Affairs Manual Volume 5 Handbook 2 Telecommunications Handbook for more info)

Non Disclosure Agreement

Note that this determination about unsworn statements of Official Classification Authority (OCAs) by the Investigating Officer Lt. Col. Paul Almanza formed one of four bases for the Defense's Motion for the Investigating Officer Lt. Col. Paul Almanza to Recuse himself

OCA CLASSIFICATION REVIEW Additionally on 17 November 2011 the Government provided the Defense with the four-page GTMO classification review completed on 4 November 2011.

Finally the Defense was provided with two classification reviews on 12 December 2011: a three-page Central Intelligence Agency (CIA) (Government Agency) classification review and a 12-page Central Intelligence Agency (CIA) (Government Agency) classification review

OCA CLASSIFICATION REVIEW Beginning on 24 October 2011 the long-awaited OCA classification reviews began to trickle in. The Government provided the Defense with the Defense Information Systems Agency (DISA) classification review on 24 October 2011

OCA CLASSIFICATION REVIEW The Government also provided a 28-page Central Intelligence Agency (CIA) (Government Agency) classification review to the Defense on 4 November 2011 Central Intelligence Agency (CIA) (Government Agency) classification review and its disclosure to the Defense

OCA CLASSIFICATION REVIEW The Government provided a few more classification reviews to the Defense on 8 November 2011. This round of disclosure included a three-page CENTCOM PowerPoint classification review that was completed on 21 February 2011 A 24-page CENTCOM classification review that was completed on 21 October 2011 A four-page CYBERCOM classification review that was completed on 21 July 2011 and a 51-page Department of State classification review that was completed on 30 October 2011. The Government did not explain the reason for the eight-plus month delay between the completion of the CENTCOM PowerPoint classification review and its disclosure or the reason for the three-plus month delay between the completion of the CYBERCOM classification review and its disclosure

OCA CLASSIFICATION REVIEW The Government provided the three-page Apache Video classification review which was completed on 26 August 2010 to the Defense on 4 November 2011. The Defense received no explanation for the delay of over a year and two months between the completion of this classification review and its disclosure to the Defense

OCA CLASSIFICATION REVIEW The Government provided the three-page Apache Video classification review which was completed on 26 August 2010 to the Defense on 4 November 2011. The Defense received no explanation for the delay of over a year and two months between the completion of this classification review and its disclosure to the Defense. OCA CLASSIFICATION REVIEW The Government also provided a 28-page Central Intelligence Agency (CIA) (Government Agency) classification review to the Defense on 4 November 2011

OCA testimony went to the heart of one of the elements of the charged offenses

Office 26 of the Military Commissions Act

Office of Counterintelligence and Consular Support in the Bureau of Intelligence and Research at the Department of State (State Department) (DoS)

Office of Naval Intelligence

Office of the Director of National Intelligence (ODNI)

Office of the Director of National Intelligence (ODNI) CENTAUR Logs (NetFlow Logs)

Office of the Director of National Intelligence (ODNI) Classification Review

Office of the Director of National Intelligence (ODNI) Keyword Search Logs

Office of the Director of National Intelligence (ODNI) The Government intends to use information from this Department during its case-in-chief

Office of the National Counterintelligence Executive (ONCIX)

Office of the National Counterintelligence Executive (ONCIX) damage assessment

Office of the National Counterintelligence Executive (ONCIX) The Court found in its ruling that ONCIX was a closely aligned agency

on 10 December 2010 Capt. Hoder forensic psychiatrist for the Quantico brig recommended that I remain under POI watch for one week the following week he once again recommended to CW4 James Averhart that I be removed from POI watch

on 13 September 2012 the Government responded 66 days after request saying "The Quantico video (Referenced in Bates Number 00042936) does not exist

on 15 March 2012 Article 38(a) Session Judge Lind recited a synopsis of the RCM 802 conference. When the Government spoke about Brady search the Government said they had not found any Brady material even though they looked for a year. Fen (Prosecution) Correct. Evolving...

on 16 April 2012 then-CPT Fen sent an email to Mr. Coombs explaining that of the 14 hard drives referenced in the Defense's 21 September 2011 Discovery Request and the Court's 23 March 2012 ruling on the Defense Motion to Compel 2 drives were completely inoperable 7 drives were wiped and 1 drive was partially wiped...The email did not state when the 8 drives were wiped

on 16 January 2012 the Defense filed another Request for Oral Deposition naming two additional Original Classification Authority (OCAs)

on 16 November 2011 the Government notified the Defense and the Article 32 Investigating Officer (IO) that the Special Court-Martial Convening Authority (SPCMA) had ordered the restart of the Article 32...The SPCMA ordered the Article 32 to start no earlier than thirty days from 16 November and to conclude no later than sixty days from 16 November...Given the Government's failure to respond to the Defense's requests filed on 13 May 2011 21 September 2011 13 October 2011 15 November 2011 and 16 November 2011 the Defense filed a Defense Request for Production of Evidence with the Article 32 Investigating Officer Lt. Paul Almanza

on 18 January 2011 over the recommendation of Capt. Hoder forensic psychiatrist for the Quantico brig and the defense psychiatrist Capt. Brian Moore former Quantico Brig Commander CW4 Averhart placed me under suicide risk

on 2 December 2011 the Defense submitted its witness list to the Article 32 Investigating Officer naming the seven Original Classification Authority (OCAs) as witnesses and explaining in detail the relevance of each of the Original Classification Authority (OCA)s testimony. At the time there were seven identified Original Classification Authority (OCA)s. A subsequent Original Classification Authority (OCA) was requested as soon as his identity was known to the Defense

on 20 May 2009 [NOTE DATE. SAME TIME video] folder BE22PAX.zip created; a large number of files were downloaded and compressed into a .zip file. These included .jpg images of presentations and documents from hospital burn victims. Special Agent David Shaver Computer Crimes Investigation Command (CCIU) did not examine this .zip file because it was no longer present on the Alienware .22 computer

on 22 March 2012 statement to the Court the Government stated "the United States is concurrently working with other Federal Organizations which we have a good faith basis to believe may possess damage assessments or impact statements..." See Prosecution's Response to Court's Email Questions (22 March 2012)

on 23 March 2012 the Court granted the Defense Motion to Compel Discovery in part with regard to the 14 hard drives from the Tactical Sensitive Compartmented Information Facility (T-SCIF) and the Tactical Operations Center (TOC) of Headquarters and Headquarters Company (HHC) 2nd Brigade Combat Team (BCT) 10th Mountain Division Forward Operating Base (FOB) Hammer Iraq

on 23 March 2012 the Court granted the Defense Motion to Compel Discovery in part with regard to the 14 hard drives from the Tactical Sensitive Compartmented Information Facility (T-SCIF) and the Tactical Operations Center (TOC) of Headquarters and Headquarters Company (HHC) 2nd Brigade Combat Team (BCT) 10th Mountain Division Forward Operating Base (FOB) Hammer Iraq The Court Ordered the Government to immediately cause an inspection of the 14 hard drives for the presence of Wget

on 24 May 2012 MAJ Fen wrote to the General Counsel at Office of the National Counterintelligence Executive (ONCIX)

on 29 July 2011 the Government sent out a memo to Headquarters Department of the Army requesting it to task Principal Officials to search for and preserve any discoverable information

on 6 June 2012 the Government provided Defense with oral notification of the existence of the DHS damage assessment

on April 19 2011 a day before Bradley Manning's unexpected transfer to Fort Leavenworth defense reported finding out about a January 13 2011 secret high-level meeting and suspected their

knowledge of the meeting may have led to the Department of Defenses' about-face on Manning's illegal pretrial confinement

On April 24 2012 the Government produced the Department of State damage assessment for in camera review

On August 6 2010 one of these mental health professionals determined that PFC Manning was no longer a suicide risk

On December 10 2010 Capt. Hocter forensic psychiatrist for the Quantico brig recommended that I remain under POI watch for one week the following week he once again recommended to CW4 James Averhart that I be removed from POI watch

On January 13 2011 secret meeting involving high-level Quantico officials where it was ordered that PFC Manning would remain in maximum custody and under prevention of injury watch indefinitely

on January 13 2011 secret meeting involving high-level Quantico officials where it was ordered that PFC Manning would remain in maximum custody and under prevention of injury watch indefinitely

on January 15 2011 Defense had filed the original Article 138 request one day after Manning was placed under "suicide risk" which resulted in his remaining in his cell for 24 hours a day and being stripped of all clothing with the exception of his underwear. His eyeglasses were also removed which left him as he describes in "total blindness". According to defense documents the stripping and interrogation that Manning endured was videotaped by the Quantico facility

on March 2 2011 PFC Bradley Manning then confined under Maximum custody and Prevention of Injury Watch (POI) at Quantico where he had been since July 29 2010 was told that his Article 138 request to be placed under Medium custody and removed from harsh and punitive pretrial confinement was denied by Daniel J. Chole

On May 31 2012 the Government provided notice to the Court and the Defense that QNCIX had a draft damage assessment Along with the Government's notice it provided a copy of its 24 May 2012 letter to QNCIX and the reply by QNCIX on 30 May 2012

on November 22 2011 defense also filed the following request for the production of evidence of the Quantico video of Manning being stripped and interrogated

Open Source Center Logs

Original Classification Authority (OCA)

Other unspecified log files that Special Agent David Shaver Computer Crimes Investigation Command (CCIU) said hundreds of thousands of other files being downloaded at the same time

Package of Bradley Manning's personal belongings from Camp Arifjan sent to his aunt Debra Van Aalstyne

partment of State (State Department) (DoS) briefing of House and Senate on December 2 2010

Patricia Williams

Patrick Kennedy Undersecretary for Management at the Department of State

Patrick Kennedy Undersecretary for Management at the Department of State briefed Congress in late November and early December of 2010 about WikiLeaks

Patrick Kennedy Undersecretary for Management at the Department of State testimony before Senate Committee on Homeland Security and Governmental Affairs in March of 2011

Paul Kaminski President's Intelligence Advisory Board

PFC Manning had full authority to access the government computer(s) at issue and at no time did he obtain or alter information that he was not entitled to obtain or alter

PFC Manning's cellular telephone

PFC Manning's RCM 707 speedy trial rights have been violated

Plc. Manning allegedly signed seven Non Disclosure Agreements (NDAs)

Philip Zelkow President's Intelligence Advisory Board

PJ Crowley former spokesperson for the Department of State (State Department) (DoS)

Portion of the Excel spreadsheet display of the CENTAUR log data for the Alienware 22 or Dell 40 machines connections to the CENTCOM CIDNE database in Tampa FL

Portion of the Excel spreadsheet display of the CENTAUR log data for the Alienware 22 or Dell 40 machines connections to the SOUTHCOM GTMO server

Portion of the Excel spreadsheet displayed in Court of the CENTAUR log data for the Alienware 22 or Dell 40 machines connections to the Department of State (State Department) (DoS) NetCentric database

President Barack Obama

President Barack Obama 21 January 2009 FOIA and Transparency and Open Government memoranda

President Barack Obama 29 December 2009 Executive Order 13526

President Barack Obama 8 December 2009 Open Government Directive (OGD)

President Barack Obama Reducing Over-Classification Act on 7 October 2010

President Barack Obama statements about CIDNE (Combined Information Data Network Exchange) Afghanistan

President Obama issued Executive Order (EO) 13587 "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information" on 7 October 2011

President's Chief of Staff formerly William Daley

President's Chief of Staff Jacob Lew

President's Daily Brief (PDB)

President's Intelligence Advisory Board

President's National Security Advisor Thomas E. Donilon

President's National Security Council's Interagency Process (IAP)

Primary lead for WikiLeaks investigation was Camp Liberty Army Criminal Investigation Command (CID) and the Department of State (State Department) (DoS). Then the Federal Bureau of Investigation (FBI)

Prosecution's notice to the Court of the computer forensics regarding the programs and the music and the videos that was not authorized on the Government computer

Protective Order

Quantico base commander

Quantico Brig Commander Chief Warrant Officer Denise Barnes

Quantico Brig Commander Chief Warrant Officer Denise Barnes used my sarcastic comment as justification to increase the restrictions imposed upon me under the guise of being concerned that I was a suicide risk

Quantico Brig Incident Report on 13 March 2011

Quantico Duty Brig Supervisor on 13 March 2011

Quantico suicide prevention blanket

22 April 2011. See id. ""Redacted"" explained that this delay was necessary because of the Board's "limited availability to meet as a full board to discuss the report. This is because of conflicting schedules and demands of the three board members"

Redacted person with whom Sergeant (former Specialist) Daniel Padgett worked on the night-shift with in addition to then Pfc. Manning

REDACTED PFC Manning filed numerous complaints about his pretrial confinement and requests to have his confinement conditions reconsidered - a complaint with the ""Redacted""""Redacted"" A DD Form 510 completed through the Brig's grievance process A request for release from pretrial confinement under RCM 305(g) a request for redress under Article 138 and two rebuttals of the inadequate responses to this request to be precise - all to no avail

REDACTED The ""Redacted""""Redacted""""Redacted"" approved of the Duty Brig Supervisor's Maximum (MAX) custody determination and also decided that PFC Manning should be placed under special handling instructions of Suicide Risk (SR) Suicide Risk (SR) Despite the recommendations of two senior forensic psychologists (and contrary to the requirements of Secretary of War Instruction (SECNAVINST) 1640-01 the Brig did not immediately remove PFC Manning from Suicide Risk-waiting almost a full week to move PFC Manning from Suicide Risk to Prevention of Injury (POI) status on 11 August 2011 For the next 8 months PFC Manning remained in MAX custody and POI status despite the recommendations of multiple psychiatrists that he be downgraded from POI status PFC Manning under MAX custody and POI status he was placed on Suicide Watch on two separate occasions from 18 January 2011 to 21 January 2011 and from 2 March 2011 until the time he was transferred to the Joint Regional Correctional Facility (JRCF) at Fort Leavenworth Kansas on 20 April 2011

REDACTED The Defense requested a copy of the video of PFC Manning being ordered to surrender his clothing at the direction of CW4 JAMES AVERHART FORMER QUANTICO BRIG COMMANDER and the subsequent interrogation by FOUR UNARMED GUARDS

REDACTED The Defense requested a copy of the video of PFC Manning being ordered to surrender his clothing at the direction of CW04 JAMES AVERHART FORMER QUANTICO BRIG COMMANDER and the subsequent interrogation by FOUR UNARMED GUARDS

REDACTED The Department of Defense (DOD) reached out for assistance from the Department of State (State Department) Federal Bureau of Investigation (FBI) Defense Intelligence Agency (DIA) Office of the National Counterintelligence Executive (ONCIE) and Central Intelligence Agency (CIA). The Defense argued that it was entitled to receive all forensic results and investigative reports by any of the cooperating agencies in this investigation. Additionally the Defense noted that ROBERT GATES FORMER SECRETARY OF DEFENSE on 29 July 2010 directed the Defense Intelligence Agency (DIA) to lead a comprehensive review of the documents allegedly given to WikiLeaks and to coordinate under the Information Review Task Force (IRTF) formerly TF 725 to conduct a complete damage review. The Defense believed based upon public acknowledgements by representatives of the Government that the results of this damage review would under the testimony of each the Original Classification Authority (OCA) for the charged documents. Specifically based upon public documents it appeared that the Information Review Task Force (IRTF) concluded that no sources or methods were revealed by the alleged disclosures and that all of the information allegedly disclosed was either dated represented low-level opinions or was already commonly understood and known due to previous public disclosures

REDACTED The Department of State (State Department) (DoS) formed a task force of over 120 individuals to review each released diplomatic cable. The task force conducted a damage assessment of the leaked cables and concluded that the information leaked either represented low-level opinions or was already commonly known due to previous public disclosures. According to published reports in multiple news agencies including the Associated Press The Huffington Post and Reuters internal US government reviews by the Department of Defense and the Department of State determined that the leak of diplomatic cables caused only limited damage to US interests abroad. According to the published account "[a] congressional official briefed on the reviews stated that the administration felt compelled to say publicly that the revelations had seriously damaged American interests in order to bolster legal efforts to shut down the WikiLeaks website and bring charges against the leakers." The official is quoted as saying "we were told (the impact of WikiLeaks revelations) was embarrassing but not damaging." This determination was at odds with the classification review conducted by the Original Classification Authority (OCA). As such the Defense argued that XXXXXXXXXXXX should not be permitted to espouse is inconsistent with the damage assessments conducted by the government

REDACTED The DOJ has conducted a very public investigation of WikiLeaks as referenced by XXXXXXXXXXXX The Defense requested any grand jury testimony and any information relating to any 18 USC 2703(d) order or any search warrant by the government of Twitter Facebook Google or any other social media site that was relevant to PFC Bradley Manning

REDACTED The Government acknowledges that the FBI in this case participated in a joint investigation of the accused. It also acknowledges that the DOJ is closely aligned in that XXXXX (long redaction)

REDACTED The Government produced the Quantico video of PFC Manning being ordered to surrender his clothing but not the video of the subsequent interrogation by CW4 James Averhart Quantico Brig Commander At the 15 March 2012 Article 39(a) Session the Government said the video of CW4 Averhart did not exist

REDACTED The Government produced the Quantico video of PFC Manning being ordered to surrender his clothing but not the video of the subsequent interrogation by CW04 James Averhart Quantico Brig Commander At the 15 March 2012 Article 39(a) Session the Government said the video of CW04 Averhart did not exist

REDACTED Three civilian Original Classification Authority (OCAs) one of them is Mr. Betts US CYBERCOM Chief Classification Officer classification determination for "The alleged chat logs" Ambassador Patrick Kennedy Undersecretary for Management at the Department of State who reviewed the disclosure of Department of State Diplomatic Cables stored within Net Centric Diplomacy server and part of SPROS Robert Rowland

REDACTED Three Original Classification Authority (OCAs) the Government refused to provide the contact info for are Ambassador Patrick Kennedy Undersecretary for Management at the Department of State Robert Rowland and Mr. Betts US Cyber Command Chief Classification Officer

REDACTED Two individuals (2) who Sergeant (former Specialist) Daniel Padgett said in his sworn affidavit gave permission to handle disciplinary actions for PFC Manning

REDACTED Unknown Army CCUI Agent no. 7 on 3 December 2011 Defense Request for Article 32 Witnesses XXXXXXXXXXXX [WHO IS THIS?] is one of the agents that worked extensively on this case for CCUI to include interviewing multiple witnesses in the case and conducting field investigation for the CCUI. XXXXXXXXXXXX [WHO IS THIS?] will testify about his involvement in the case and the investigative steps that he took

REDACTED Unknown Diplomatic Security Services (DSS) at the Department of State (State Department) (DoS) Agent No. 8 on 2 December 2011 Defense Request for Article 32 Witnesses XXXXXXXXXXXX [WHO IS THIS?] is one of the law enforcement agents that conducted work on this case. The defense requests that XXXXXXXXXXXX [WHO IS THIS?] be instructed to provide the Investigating Officer (LI Col. Paul Almaraz) and the defense with a complete copy of DSS Diplomatic Security Services at the Department of State (State Department) (DoS) case file number XXXXXXXXXXXX [WHAT IS THIS NUMBER?] and any other collateral investigations by the DSS Diplomatic Security Services at the Department of State (State Department) (DoS) related to this case at least two weeks prior to the start of the Article 32 hearing

REDACTED With the exception of James Cully 4th Cavalry Division Brigade S2 is the Official Classification Authority for classification review of the unclassified July 12 2007 Baghdad airstrike videos also known as "Collateral Murder" the Government did not deny that the testimony of the Original Classification Authority OCA was relevant relating to the national defense

Rene Bitter director of the Operations Center (S/ES-O) at the Department of State (State Department) (DoS)

Representative of the United States of American to the United Nations Susan Rice

Reykjavik 13

Richard Danzig President's Intelligence Advisory Board

Rita Hauser President's Intelligence Advisory Board

Robert Boback Chief Executive Officer of Tiversa Inc. a Federal Bureau of Investigation (FBI) contractor

Robert Gates Former Secretary of Defense

Robert Gibbs White House Press Secretary

Robert Rowland

Roel Campos President's Intelligence Advisory Board

Rogers Channel (Use ROGER CHANNEL for communications between the Assistant Secretary for Intelligence and Research (NIR) and the chief of mission See US Department of State (State Department) (DoS) Foreign Affairs Manual Volume 5 Handbook 2 Telecommunications Handbook for more info)

Ronald L. Burgess former director of the Defense Intelligence Agency

Rob Gonggrip

Rob Gonggrip Twitter

Russell Travers National Security Staff Senior Advisor for Information Access and Security

Sadler (sp.)

SD card allegedly obtained during the second search of Debra Van Alstyne Bradley Manning's aunt home after having allegedly been shipped from Iraq in October 2010

SD card collected from Bradley Manning's Debra Van Alstyne home apparently sent from Iraq

Secretary of Energy Steven Chu

Secretary of Homeland Security Janet Napolitano

Secretary of State Hillary Clinton

Secretary of State Hillary Clinton attended the Organization for Security and Cooperation in Europe (OSCE) which was the main focus the 24/7 WikiLeaks Working Group namely staying ahead of the news cycle

Secretary of the Army John McHugh

Secretary of the Army's 15-6 investigation

Section 3 "type files"

Senator Carl Levin Chair of the Senate Armed Services Committee

Sergeant (former Specialist) Daniel Padgett

Sergeant (former Specialist) Daniel Padgett testified that he was never Pfc. Manning's direct supervisor although he was Pfc. Manning's supervisor on the night-shift and that he was not in Pfc. Manning's chain of command. Sergeant (former Specialist) Daniel Padgett testified that despite him not being in Pfc. Manning's chain of command he did request to counsel Manning when he saw an alleged incident in December 2009 with Pfc. Manning on the night-shift. Sergeant (former Specialist) Daniel Padgett testified that during that counseling session on the importance of being on time in the (Major Clause) Brigade S2's office in the T-SCIF at FGB Hammer Pfc. Manning allegedly "was staring at me" and Sergeant (former Specialist) Daniel Padgett testified that he asked Pfc. Manning not to do that "because it made me uncomfortable". Sergeant (former Specialist) Daniel Padgett testified that Pfc. Manning allegedly "turned the table upside down and was restrained by an S2 officer [Chief Warrant Officer Four (CW4) Airman (sp.)]". Sergeant (former Specialist) Daniel Padgett testified that after Pfc. Manning allegedly flipped the table over everything hit the ground. Sergeant (former Specialist) Daniel Padgett testified that he allegedly moved Pfc. Manning away because Sergeant (former Specialist) Daniel Padgett testified he saw there were weapons. Sergeant (former Specialist) Daniel Padgett testified that the officer in charge Chief Warrant Officer Four (CW4) Airman (sp.) restrained Pfc. Manning by sitting him on a bench and telling Pfc. Manning to sit. Sergeant (former Specialist) Daniel Padgett testified that during the alleged December 2009 incident "We cleared the room." Reitman notes that Sergeant (former Specialist) Daniel Padgett testified that "two computers and a radio crashed to the ground". Sgt. Padgett put his hand on PFC Manning to calm him down. Moments later the Chief Warrant Officer [Four (CW4) Airman (sp.)] put PFC Manning in a "full nelson" style wrestling head lock. Sergeant (former Specialist) Daniel Padgett testified that he spoke to a few people in the brigade about the incident but that he did not talk to Master Sergeant (not Sergeant First Class) Adkins Major Clause the First Sergeant or Company Commander Drew (sp.). Sergeant (former Specialist) Daniel Padgett testified that there was no UCMJ [Uniform Military Code of Justice] action received by Pfc. Manning due to the incident in December 2009. Showman testified that her desk was outside the entrance to the T-SCIF conference room. Specialist Jihfeah Showman testified however that she heard Manning scream and she got up and went to the door of the conference room. Specialist Jihfeah Showman testified to an early May 2009 incident with Bradley Manning before deployment. Showman testified that Bradley Manning missed PT formation and Showman went to the barracks to find out where Bradley Manning was. When she knocked on Bradley Manning's door Manning opened it and Showman testified that Manning looked like he had just woken up. Showman said that Manning was dressed in civilian clothes. Showman testified that she told Manning that "he needed to get dressed and get downstairs." Once Manning got into uniform she talked to Manning as she walked with him back to formation. She asked him "How he had slept why he wasn't at formation was it an alarm situation? Why hadn't he shown up?" Showman testified that Manning did not respond to anything that Showman said to him. Showman told Manning she would have to counsel him and that he would have to show up early for a couple weeks for correction. When they came upon Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) Showman testified that Manning allegedly started screaming at the top of his lungs and saliva was coming out of his mouth. Showman testified that Manning was allegedly swinging his arms around. At that point Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) approached Manning and Manning allegedly stopped. Showman testified that Manning's fists were allegedly still clenched and Manning continued to make grunting noises. Showman testified that when Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) asked Manning what was wrong Manning said that he could not take messing up that he "hated messing up." Showman testified that she recommended counseling because Manning lost his "military bearing" and Showman set up a meeting with Manning. According to Showman's testimony no one alerted the Company Commander at Fort Drum NY and no one recommended a behavior evaluation. Showman testified that she recommended further action to Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) and that she told Adkins that Manning was a threat to himself and others that Manning should not have classified actions and that Showman thought that Manning should not deploy. Showman testified that Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) did not pass any of that information along. Showman testified that she knows that Adkins said something to the S2 Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action).

Sergeant Chad Madaras

Sergeant Chad Madaras and Bradley Manning were opposite shifts until late in deployment when they switched and Manning worked the day and Madaras at night. They both worked on the "Shia Threat". They shared an Alienware and a Dell 6300 computer

Sergeant Chad Madaras met Bradley Manning at Fort Drum in 2008

Sergeant Chad Madaras recounts how Warrant Officer One (WO1) Kyle Balones, and Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) called Bradley Manning's name trying to get his attention and Bradley Manning just stared at his screen unresponsive

Sergeant Chad Madaras thought mIRC was mission critical

Sergeant Chad Madaras was with Bradley Manning at Joint Readiness Training Center (JRTC)

Sergeant First Class Brian Madrid Platoon Sergeant Fort Huachuca

SF312

SIDOCF [Security Investigations Division/ Central Clearance Facility]

Since 2 March 2011 I have been stripped of all my clothing at night I have been told that the PCF Commander Chief Warrant Officer Denise Barnes intends on continuing this practice indefinitely

So the Government is saying that there are 250000 pages in its possession custody and control that relate to the accused Wikileaks and/or the damage occasioned by the leaks that it has not produced to the Defense?

Something the defense describes as a Farah file in the unallocated space but it is not mentioned by either Reitman or transcriber at any other time. Nor is it clear on which computer (either the Dell .40 or Alienware .22) or where this reference was found

Sonic

SOUTHCOM

Spear fishing

Special Agent Aims Army Computer Crimes Investigation Command (CCU) acting Operations Officer and Special Agent Mark Mander's supervisor

Special Agent Alfred Williamson CCU

Special Agent Antonio Patrick Edwards Army Computer Crimes Investigation Command (CCU)

Special Agent Antonio Patrick Edwards Army Computer Crimes Investigation Command (CCU) testified that Adrian Lamo was a confidential informant for the Army Criminal Investigation Command (CID) beginning in the latter part of July 2010 until August or September of 2011

Special Agent Antonio Patrick Edwards Army Computer Crimes Investigation Command (CCIU) testified that his first contact with Adrian Lamo was on 25 May 2010 when Uber connected Edwards to Lamo. Edwards testified that the only other time(s) he communicated with Lamo after that was to set up a meeting date Edwards testified that he came into physical contact with Lamo on June 11 2010 when Edwards met with Lamo in Carmichael CA

Special Agent Antonio Patrick Edwards CCIU testified that Adrian Lamo was a confidential informant for the Army Criminal Investigation Command beginning in the "latter part of July 2010" until August or September of 2011

Special Agent Antonio Patrick Edwards CCIU testified that he attempted to interview Danny Clark between 18 and 23 June 2010 but that he did not interview Clark because Clark invoked his right to counsel

Special Agent Antonio Patrick Edwards CCIU testified that he had knowledge that Danny Clark communicated with Adrian Lamo because Adrian Lamo provided Edwards with the chat log between Lamo and Clark "around July 22 [2010]"

Special Agent Calder Robertson CCIU

Special Agent Calder Robertson CCIU collected hard drives another unnamed special agent did everything else

Special Agent Calder Robertson CCIU extracted the hard drives from the two SIPR and one NIPR computers collected from the SCIF the personal laptop of Staff Sergeant Peter Bigelow Supply Room and the personal external hard drive of PFC Manning and can testify concerning the forensic imaging and evidence collection of electronic media seized in Iraq

Special Agent David Shaver Computer Crimes Investigation Command (CCIU)

Special Agent David Shaver Computer Crimes Investigation Command (CCIU) found 4 complete Gilmo detainee assessments zero files were found in the unallocated space despite Special Agent David Shaver's Computer Crimes Investigation Command (CCIU) assertion that Manning appeared to have downloaded hundreds of Guantanamo detainee assessments

Special Agent David Shaver Computer Crimes Investigation Command (CCIU) in sworn testimony that the Microsoft PowerPoint file "Farah brief final version" alleged to have been downloaded by the Alienware 22 SIPRNet computer on 10 April 2010 at 13:12:24 hours was authorized for download on SIPRNet machines which means the document would have to be SECRET or below

Special Agent David Shaver's Computer Crimes Investigation Command (CCIU) testified that CENTCOM logs evidence only one PowerPoint file "Farah brief final version" was downloaded by the Alienware 22 computer on 10 April 2010 at 13:12:24 hours

Special Agent Johnson Army Computer Crimes Investigation Command (CCIU) who did analysis of media from Iraq

Special Agent King Army Computer Crimes Investigation Command (CCIU) acting Operations Officer who did search authorization interviews and administrative tasks

Special Agent Mark Mander Army Computer Crime Investigative Unit (CCIU) case agent

Special Agent Mark Mander Army Computer Crime Investigative Unit (CCIU) says Adrian Lamo's initial information started the investigation

Special Agent Mark Mander Army Computer Crime Investigative Unit (CCIU) says he doesn't believe Army Computer Crimes Investigation Command (CCIU) directed Jason Katz. That was FBI

Special Agent Mark Mander Army Computer Crime Investigative Unit (CCIU) says there was a great deal of concern about a foreign intelligence service. They were looking for information to prosecute

Special Agent Mark Mander Computer Crimes Investigation Command (CCIU) testified that Lamo started to cooperate with Army Criminal Investigation Command (CID) "probably at the end of May 2010"

Special Agent Schaller Army Computer Crimes Investigation Command (CCIU) who did analysis of media from Iraq

Special Agent Toni Graham Army CID 102nd Military Police detachment

Special Agent Toni Graham Army CID 529/10 affidavit

Special Agent Toni Graham Army CID 529/10 affidavit stated Manning had been penetrating mil and gov accounts for over a year (Manning was only deployed since November 2009) but was based on information from a confidential informant

Special Agent Toni Graham Army CID discussed the confidential informant who provided them with information noting that he was in direct contact with the FBI

Special Agent Toni Graham Army CID primary duties were to protect collect and preserve digital device evidence

Special Agent Toni Graham Army CID said the information that Collateral Murder was classified (it wasn't) had come by way of the confidential informant

Special Agent Toni Graham Army CID signed 529/10 affidavit that stated Manning had released T-SGIF information and cables onto the Internet. She admitted that much of her affidavit was based on information from commanders at Ft. Belvoir who had received intelligence from a confidential informant

Special Agent Toni Graham Army CID testified that she'd received authorization to seize and search the devices via her commander as well as with consent from Staff Sergeant Peter Bigelow and also through formal search authorization granted to her

Special Agent Toni Graham Army CID was serving on a battalion in Baghdad on 27 May 2010 when she received instructions from her headquarters based on information from an unnamed confidential informant

Special Agent Toni Graham Army CID was the first lead agent on the case

Special Agent Troy Bettencourt Army Criminal Investigation Command (CID)

Special Agent Troy Bettencourt Army Criminal Investigation Command (CID) says on "20th of August the entire document 250000 US State Department un-redacted cables were published on the Internet"

Special Agent Troy Bettencourt Army Criminal Investigation Command (CID) testified that he interviewed 10 people including Bradley Manning's Chain of Command and contractors

Special Agent Troy Bettencourt Army Criminal Investigation Command (CID) testified that Pfc. Manning was not tied to a known terrorist group

Special Agent Troy Bettencourt Army Criminal Investigation Command (CID) that concerning the "value of information" Wikileaks has dissension within their ranks: "Mr. Assange... said folks he demanded that they sign an NDA saying they would not disclose... to Wikileaks. They said somewhere between 12 and 15 million. The valuation of information 12 million pounds [for everything they have]"

Special Agent Troy Bettencourt Army Criminal Investigation Command (CID) was on the investigation's intrusion team

Special Agent Wilbur Army Computer Crimes Investigation Command (CCIU) who analyze the path to Garani

Special Court Martial Convening Authority (SCMCA)

Specialist Eric Baker 62nd Military Police Detachment Army Criminal Investigation Command (CID) Manning's roommate at FOB Hammer Containerized Housing Unit (CHU)

Specialist Eric Baker 62nd Military Police Detachment Army Criminal Investigation Command (CID) Manning's roommate at FOB Hammer Containerized Housing Unit (CHU) admitted that if a soldier wanted to have a CD with music or photos of your family and friends in the T-SGIF they could have

Specialist Jihreah Showman

Specialist Jihreah Showman deployed to Iraq with Bradley Manning when they left Fort Drum NY on 11 Oct 2009

Specialist Jihreah Showman said that Bradley Manning received two separate TDY's [Temporary Duty Assignment] classified under SECRET at Fort Drum and Washington DC

Specialist Jihreah Showman said that Bradley Manning was a Shia analyst. Showman said that any information traffic that came in was disseminated to the Shia analysts who mined the data for information using the DSGS [pronounced "desigs" Distributed Common Ground System] machines. Analysts would create presentations for officers to give to the Brigade Commander. Analysts could search by keyword and the system had targeting folders for specific individuals. Analyst would input individual names incidents and specific dates. Analysts in the T-SGIF would go through HUMINT [Human Intelligence] reports and gather pertinent information. According to Showman analysts had "targeting packets" on every Shia and Sunni individual that came across an analysts desks which stored was on the T-SGIF shared drive

Specialist Jihreah Showman testified about a May 7 2010 incident between 8:00 p.m. and 10:00 p.m. around shift change in the conference room of the T-SGIF where she said she saw Bradley

Manning curled into a ball on the floor in the fetal position. Showman testified that she reported the incident to CW4 (Chief Warrant Officer 4) Arisman and told Arisman "Be ready for something to happen again." Showman testified after seeing the incident she told the T-SGIF because it was the end of her work day. Showman testified that on May 8 2010 at around 12:00 a.m. or 1:00 a.m. Showman was awoken and called back to the T-SGIF. Captain Casey Martin (now Captain Casey Fulton) testified that she called Specialist Jihreah Showman back to the T-SGIF. Showman testified that she was allegedly assaulted by Bradley Manning. Showman testified that after Bradley Manning allegedly assaulted her Showman pinned Manning to the ground. Showman testified that after she pinned Manning to the ground Manning said "I'm tired of this." Showman testified that Manning also said that he was scared Behavioral health would find out about him and that if they found out they would remove him from the Army.

Specialist Jihreah Showman testified about another alleged incident with Bradley Manning and a Lieutenant where the Lieutenant asked Bradley Manning to freeze and Manning was unresponsive. Showman testified that she asked Manning if something was wrong and he did not speak. Showman testified that she reported the incident to Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) and that she and Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) sat down with Bradley Manning to talk to him. Showman testified that during that conversation Bradley Manning told her and Adkins that he felt paranoid and that Manning felt that people were listening in on his conversations. Showman testified that she asked Bradley Manning if he wanted to hear himself and Manning said he was not suicidal but he felt paranoid because people were listening to him and watching his every move. Showman testified that she asked Bradley Manning if he heard voices in his head and Bradley Manning told Showman that he did not. Showman testified that based on this conversation she felt that Bradley Manning had a high level of paranoia.

Specialist Jihreah Showman testified that Bradley Manning left the Brigade T-SGIF the morning of May 9 2010 after Bradley Manning allegedly assaulted Showman on May 7 2010. Showman said that Bradley Manning "punched me in the face unprovoked".

Specialist Jihreah Showman testified that Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) did not exercise control over the soldiers in the S2 section. Specialist Jihreah Showman testified that she was a CW4 (Chief Warrant Officer Two) David Hack but that the only person that Showman had access to was Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) and that counseling for Showman was not available. Showman testified that she stopped fighting for counseling and that she was only consulted once Showman testified that she was a witness to the December 2009 incident with Bradley Manning and Sergeant (former Specialist) Daniel Padgett. Showman testified that her desk was outside the entrance to the T-SGIF conference room. Showman testified that she heard Manning scream and she got up and went to the door of the conference room. Showman testified that she saw Manning sitting on one side of the table and Sergeant (former Specialist) Daniel Padgett was sitting on the other side. Showman testified that she saw Bradley Manning allegedly flip the conference room table and that she saw a computer get broken. Showman testified that she saw Sergeant (former Specialist) Daniel Padgett stand up and move toward the table. Showman testified that she saw Sergeant (former Specialist) Daniel Padgett put his hand out and to talk to Manning down. Showman testified that she saw Manning allegedly look around and see an MH US Army assault rifle. Showman testified that she saw Manning allegedly reach for the rifle. Showman testified that she saw (see note) grab Bradley Manning from behind and drag Manning away. (NB: This was not the reason for my own Relief from Duty. I was not involved in the December 2009 incident with Bradley Manning.) Specialist Jihreah Showman testified that she saw Sergeant (former Specialist) Daniel Padgett. According to my transcript of Captain Steven Lim's testimony and Retman's transcript of Showman CW4 Warrant Officer Four (CW4) Arisman (sp.) grabbed Manning. But this transcript says that Sergeant (former Specialist) Daniel Padgett grabbed Manning. [See note] dragged Manning a couple of feet and then Manning sat. Showman testified that Manning did not receive an Article 15 (Non-Judicial Punishment). Showman testified that she spoke to Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) about the incident and told Adkins that Manning should no longer be in the T-SGIF. Showman testified that Manning was not removed. Showman testified that the December 2009 incident with Sergeant (former Specialist) Daniel Padgett should not have just remained in the S2 shop. Showman testified that the First Sergeant (WHO IS THIS?) did eventually find out because Showman's commanding officer CW2 (Chief Warrant Officer Two) Honda Hack told the First Sergeant. Showman testified that Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) did not report the incident to the First Sergeant. Showman testified that she escorted Bradley Manning to meet with the First Sergeant and that she told the First Sergeant that Manning should have never deployed and that this was not the first time and that she was not surprised about the incident.

Specialist Jihreah Showman testified that Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) was the NCDC (Non Commissioned Officer in Charge) and so it was his prerogative to close the shop who worked on the day and night shift.

Specialist Jihreah Showman testified that she barely saw Major Clausen in the S2 section and that he stayed mostly in his office.

Specialist Jihreah Showman testified that she believes that soldier and leaders have a responsibility to report matters of concern security and DEROS. Showman testified that in order to DEROS someone the Commander needs to place a recommendation and indicate what actions lead to the derogatory determination. Showman testified that the Commander checks a box indicating whether an individual can retain their security clearance of whether their clearance should be rescinded or terminated so the Brigade can deliver it to the Division.

Specialist Jihreah Showman testified that she confronted Bradley Manning when he first came to the unit that because she said he wasn't completing tasks. Showman testified that Bradley Manning told her that the reason he wasn't getting task completed was because of his paranoia of others. Showman testified that Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) told her that he reported the incident to someone. Showman testified that she recommended to Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) a command-directed referral (in order to hear from health services on what would be discussed with Manning during counseling sessions).

Specialist Jihreah Showman testified that she was the acting Security Manager in the T-SGIF and that First Lieutenant Elizabeth Fields was the Security Manager before her.

Specialist Jihreah Showman testified that when she saw Bradley Manning's name on the deployment list she was furious. When she went to Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) about his name being on the deployment list Adkins told her that Manning would be deployed and Showman would have to deal with it.

Specialist Jihreah Showman was playing July 2007 Baghdad Apache airstrike (known later as Collateral Murder) on her workstation before April 2010 when it was published by WikiLeaks.

Specialist Jihreah Showman worked with Bradley Manning in the 2nd Brigade T-SGIF at FOB Hammer Iraq which functioned as a fusion cell. Showman was in the same unit and Bradley Manning's team leader specifically she was Bradley Manning's supervisor for the first two months of deployment on the night shift. Specialist Jihreah Showman worked for the first two months of deployment with Bradley Manning on the night shift then Showman was switched to day shift. Then Manning was moved to day shift with her.

Specialist Sadler (sp.)

SPECIFICATION 1 (I): In that Private First Class Bradley E. Manning US Army did at or near Contingency Operating Station Hammer Iraq between on or about 1 November 2009 and on or about 27 May 2010 wrongfully and wantonly cause to be published on the internet intelligence belonging to the United States government having knowledge that intelligence published on the internet is accessible to the enemy such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.

SPECIFICATION 1 (II): In that Private First Class Bradley E. Manning US Army did at or near Contingency Operating Station Hammer Iraq between on or about 1 November 2009 and on or about 8 March 2010 violate a lawful general regulation to wit, paragraph 4-5p(4) (4) Army Regulation 25-2 dated 24 October 2007 by attempting to bypass network or information system security mechanisms.

SPECIFICATION 10 (I): In that Private First Class Bradley E. Manning US Army did at or near Contingency Operating Station Hammer Iraq between on or about 11 April 2010 and on or about 27 May 2010 having unauthorized possession of information relating to the national defense to wit: more than five classified records relating to a military operation in Farah Province Afghanistan occurring on or about 4 May 2009 with reason to believe such information could be used to the injury of the United States or to the advantage of any foreign nation willfully communicate deliver transmit or cause to be communicated delivered or transmitted the said information to a person not entitled to receive it in violation of 18 U.S. Code Section 793(e) such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.

SPECIFICATION 11 (I): In that Private First Class Bradley E. Manning US Army did at or near Contingency Operating Station Hammer Iraq between on or about 1 November 2009 and on or about 8 January 2010 having unauthorized possession of information relating to the national defense to wit: a file named "B222 PAX.zip" containing a video named "B222 PAX.wmv" with respect to believe such information could be used to the injury of the United States or to the advantage of any foreign nation willfully communicate deliver transmit or cause to be communicated delivered or transmitted the said information to a person not entitled to receive it in violation of 18 U.S. Code Section 793(e) such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.

Specification 11 (II): In that Private First Class Bradley E. Manning US Army did at or near Contingency Operating Station Hammer Iraq between on or about 28 March 2010 and on or about 4 May 2010 stipulate purport or knowingly cause to his use or the use of another record or thing of value of the United States or of a department or agency thereof to wit: The Department of State Net-Centric Database containing more than 250000 records belonging to the United States government of value of more than \$1000 in violation of 18 U.S. Code Section 841 such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.

SPECIFICATION 12 (I): In that Private First Class Bradley E. Manning US Army did at or near Contingency Operating Station Hammer Iraq between on or about 28 March 2010 and on or about 27 May 2010 having knowingly exceeded authorized access on a Secret Internet Protocol Router Network computer and by means of such conduct having obtained information that has been

determined by the United States government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations to wit: more than seventy-five classified United States Department of State cables willfully communicate deliver transmit or cause to be communicated delivered or transmitted the said information to a person not entitled to receive it with reason to believe that such information so obtained could be used to the injury of the United States or to the advantage of any foreign nation in violation of 18 US Code Section 1030(a)(1) such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces

SPECIFICATION 14 (II). In that Prate First Class Bradley E. Manning US Army did at or near Contingency Operating Station Hammer Iraq between on or about 15 February 2010 and on or about 18 February 2010 having knowingly exceeded authorized access on a Secret Internet Protocol Router Network computer and by means of such conduct having obtained information that has been determined by the United States government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations to wit: a classified Department of State cable titled "Rjevaykiv-13" willfully communicate deliver transmit or cause to be communicated delivered or transmitted said sensitive information to a person not authorized to receive it; and that such information was obtained could be used to the injury of the United States or to the advantage of any foreign nation in violation of 18 USC Code Section 1303(a) (1) such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.

SP5CIFICATION 15 (II). In that Private First Class Bradley E. Manning US Army did at or near Contingency Operating Station Hammer Iraq between on or about 15 January 2010 and on or about 15 March 2010 having unauthorized possession of information relating to the national defense to wit: a classified record produced by a United States Army intelligence organization dated 18 March 2008 with reason to believe such information could be used to the injury of the United States or to the advantage of any foreign nation willfully communicate deliver transmit or cause to be communicated delivered or transmitted the said information to a person not entitled to receive it in violation of 18 US Code Section 793(e) such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces

SPECIFICATION 16 (U). In that Private First Class Brainer E. Manning US Army did at or near Congress Operating Station Hammer Iraq between on or about 11 May 2010 and on or about 27 May 2010 steal purloin or knowingly convert to his use or the use of another a record or thing of value of the United States of or a department or agency thereof to wit: The United States Forces - Iraq Microsoft Outlook / Share Point Exchange Server global address list belonging to the United States government of a value of more than \$1000 in violation of 18 US Code Section 641 such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces

SP5IFICATION 2 (II). In that Private First Class Bradley E. Manning U.S. Army did at or near Contingency Operating Station Hammer Iraq between on or about 15 February 2010 and on or about 5 April 2010 having unauthorized possession of information relating to the national defense to wit: a video file named "12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.avi" with reason to believe such information could be used to the injury of the United States or to the advantage of any foreign nation willfully communicate defense transmit or cause to be communicated delivered or transmitted the said information to a person not entitled to receive it in violation of 18 U.S. Code Section 793(e) such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces

SPECIFICATION 2 (III): In that Private First Class Bradley E. Manning US Army did at or near Contingency Operating Station Hammer Iraq between on or about 11 February 2010 and on or about 3 April 2010 violate a lawful general regulation to wit: paragraph 4-5(a)(3) Army Regulation 25-2 dated 24 October 2007 by adding unauthorized software to a Secret Internet Protocol Router Network computer

SPECIFICATION 3 (U). In that Private First Class Bradley E. Manning U.S. Army did at or near Contingency Operating Station Hammer Iraq between on or about 22 March 2010 and on or about 26 March 2010 having unauthorized possession of information relating to the national defense to wit: more than one classified memorandum produced by a United States government intelligence agency with reason to believe such information could be used to the injury of the United States or to the advantage of any foreign nation willfully communicate deliver transmit or cause to be communicated delivered or transmitted the said information to a person not entitled to receive it in violation of 18 U.S. Code Section 793(e) such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces

SPECIFICATION 3 (III): In that Private First Class Bradley E. Manning US Army did at or near Contingency Operating Station Hammer Iraq on or about 4 May 2010 violate a lawful general regulation to wit, paragraph 4-5(a)(3) Army Regulation 25-2 dated 24 October 2007 by adding unauthorized software to a Secret Internet Protocol Router Network computer

SPECIFICATION 4 (II): in that Private First Class Bradley E. Manning U.S. Army did at or near Contingency Operating Station Hammer Iraq between on or about 31 December 2009 and on or about 5 January 2010 steal purloin or knowingly convert to his use or the use of another record or record of value of the United States or of a department or agency thereof to wit: the Combined Information Data Network Exchange Iraq database containing more than 380000 records belonging to the United States government of a value of more than \$1000 in violation of 18 U.S. Code Section 641 such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces

SPECIFICATION 4 (lit): In that Private First Class Bradley E. Manning US Army did at or near Contingency Operating Station Hammer Iraq between on or about 11 May 2010 and on or about 27 May 2010 violate a lawful general regulation to wit: paragraph 4-5(a) (3) Army Regulation 25-2 dated 24 October 2007 by using an information system in a manner other than its intended purpose

SPECIFICATION 5 (II). In that Private First Class Bradley E. Manning U.S. Army did at or near Contingency Operating Station Hammer Iraq between on or about 31 December 2009 and on or about 9 February 2010 having unauthorized possession of information relating to the national defense to wit: more than twenty classified records from the Combined Information Data Network Exchange Iraq database with reason to believe such information could be used to the injury of the United States or to the advantage of any foreign nation willfully communicate deliver transmit or cause to be communicated delivered or transmitted the said information to a person not entitled to receive it in violation of 18 U.S. Code Section 793(e) such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces

SPECIFICATION 6 (U): In that Private First Class Bailey E. Manning U.S. Army did at or near Contingency Operating Station Hammer Iraq between on or about 31 December 2009 and on or about 8 January 2010 steal property or knowingly convert to his use or the use of another a record of thing of value of the United States or of a department or agency thereof to wit: Combined Information Data Network Exchange Afghanistan database containing more than 90000 records belonging to the United States government of a value of more than \$1000 in violation of 18 U.S. Code Section 641 such conduct being original, to good credit and disclosure in the armed forces and being of a nature to bring discredit upon the armed forces

SPECIFICATION 7 (II), in that Private First Class Bradley E. Manning U.S. Army did or at near Contingency Operating Station Hammer Iraq between on or about 31 December 2009 and on or about 9 February 2010 having unauthorized possession of information relating to the national defense to wit: more than twenty classified records from the Combined Information Data Network Exchange Afghanistan database with reason to believe such information could be used to the injury of the United States or to the advantage of any foreign nation willfully communicate deliver transmit or cause to be communicated delivered or transmitted the said information to a person not entitled to receive it in violation of 18 U.S. Code Section 793(e) such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.

SPECIFICATION 8 (II): in that Private First Class Bradley E. Manning U.S. Army did at or near Contingency Operating Station Hammer Iraq on or about 8 March 2010 steal purloin or knowingly convert to his use or the use of another a record or thing of value of the United States or of a department or agency thereof to wit: a United States Southern Command database containing more than 700 records belonging to the United States government of a value of more than \$1000 in violation of 18 U.S. Code Section 641 such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.

SPECIFICATION 9 (II): In that Private First Class Bradley E. Manning U.S. Army did at or near Contingency Operating Station Hammer Iraq between on or about 8 March 2010 and on or about 27 May 2010 having unauthorized possession of information relating to the national defense to wit: more than three classified records from a United States Southern Command database with reason to believe such information could be used to the injury of the United States.

States or to the advantage of any foreign nation willfully communicate deliver transmit or cause to be communicated delivered or transmitted the said information to a person not entitled to receive it in violation of 18 U.S. Code Section 793(e) such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces

SPEEDY TRIAL 845 days of pretrial confinement dwarfs the periods of pretrial confinement in any reported military case

SPEEDY TRIAL At the 23 February 2012 Arrangement Combs (Defense) stated that defense would object to a trial schedule after June 2012 and that the Government suggested August 3 2012. Combs states that that his client has been in pretrial confinement for 633 days and how many days Manning will have been in confinement if the proceeding were to occur in August 2012. Fain responded that the suggestion was "realistic trial scheduling"

Speedy Trial Barker v. Wingo Prejudice should be assessed in the light of the interests of defendants which the speedy trial right was designed to protect. (i) to prevent oppressive pretrial incarceration (ii) to minimize anxiety and concern of the accused and (iii) to limit the possibility that the defense will be impaired. The most serious is the last because the ability of a defendant adequately to prepare his case skews the fairness of the entire system

SPEEDY TRIAL Defense has found no reported military case involving a period of delay even close to the 845 delay in this case

SPEEDY TRIAL Even just one or two of those periods was improperly excluded (and the Defense maintains that all challenged periods were improperly excluded)

SPEEDY TRIAL RCM 707(a) sets forth a 120-day speedy trial clock The constitutional right to speedy trial is a fundamental right of a military accused protected by both the Sixth Amendment and Article 10

Speedy Trial Taken together the 43 days from 30 May 2010 to 11 July 2010 the 8 days from 16 December 2011 to 23 December 2011 and the 52 days from 3 January 2012 to 23 February 2012 add up to 103 days. Therefore the Government cannot dispute that 103-day speed trial clock of RCM 707(a). Of the 635 days from the day after PFC Manning was placed into pretrial confinement up to and including the date PFC Manning was arraigned 532 days have been excluded by the Convening Authority and the Article 32 IO. This Motion does not challenge 205 days of those excluded days. Subtracting those 205 unchallenged days from the 635 total days the Convening Authority and the Article 32 IO excluded 327 days of the 430 remaining days. Those exclusions amount to a total of over 76% of the 430 days. In practical terms the Convening Authority and the Article 32 IO has excluded from the R.C.M. 707 speedy trial clock over 76%

SSH file log in the home folder of Bradley Manning's MacBook Pro

Staff Sergeant Peter Bigelow Supply Room

Supplement to the Case Management Order that it requires 45-60 days to coordinate and determine if the Government will claim privilege over these items under RCM 505

Surveillance

Sworn Statement Master Sergeant Brian Paki (sp.) was turned over by the Government in response to the Defense Motion to Compel Discovery No. 1 March 2012

T-SCIF had no Standard Operating Procedures and was not accredited

Terrorist Screening Center (TSC)

That the decision to place me on Suicide Risk on 18 January 2011 was improper (CJWA James Averhart Former Quantico Brig Commander)

The 52910 affidavit also specifically mentioned an article in the Stars and Stripes military publication called "A Wiki for a World of Secrets"

The Army Criminal Investigative Command (CID) requested that the evidence be preserved in September 2010 the Defense also filed a preservation request in September 2011. The Defense has recently learned that that Government believes that most or all of the drives are not operational or have been wiped clean

The Convening Authority had long been a mere rubber stamp for the Government's many delay requests

The Court Ordered the Government to immediately cause an inspection of the 14 hard drives for the presence of Wget mIRC Google Earth movies games music and any other specifically requested program from the Defense

The Court ruled on 23 March 2010 that a complete search of the hard-drives was not material to the preparation of the defense for the charged specifications. However: the Court directed the Government to search each of the 14 hard drives [or] Wget

the current Deputy Assistant Secretary of State for the Bureau of Intelligence and Research at Department of State (State Department) (DoS)

the current Deputy Assistant Secretary of State for the Bureau of Intelligence and Research at Department of State (State Department) (DoS) became aware that Office of the National Counter Intelligence Executive (ONCE) intended to a damage damage assessment in early 2011 assessment sometimes in early 2011

The Defense again specifically requested any investigative summaries damage assessments or Original Classification Authority (OCA) determinations conducted by the United States Army (US Army Criminal Investigation Command) (CID) Department of Defense (DoD) Department of Justice (DoJ) National Security Agency (NSA) Defense Intelligence Agency (DIA) Department of Homeland Security Office of Intelligence and Analysis (DHS/ISA) Federal Bureau of Investigation (FBI) and the Bureau of Diplomatic Security (DoS) at the Department of State (State Department) (DoS)

The Defense filed a motion to compel with respect to the 1294 emails that the Government did not disclose. At that point the Government "voluntarily" turned over approximately 600 more emails that were apparently material to the preparation of the defense with no explanation as to why these were not produced earlier. The Court then reviewed the remaining 600 or so emails and determined that all but twelve were material to the preparation of the defense. Of course

The Defense had barely received basic discovery (I wasn't until 27 July 2011 that the Defense started to receive the bulk of the unclassified CID file and it was not until 4 November of 2011 the month prior to the Article 32 hearing that the Defense received any of the classified discovery) PFC Manning was languishing in a Brig under oppressive conditions. And what was the Government doing? No one knows. More detailed instances of a lack of diligence and unjustified delay are discussed below

The Defense had requested that these witnesses be present at the Article 32 requested from both the SPMCA and GCMA to depose the relevant OCA witnesses and requested contact information for the relevant OCAs

The Defense is amenable to having the Government perform a meaningful search of the computers for the requested information

The Defense requested that the Government disclose items seized by the DOJ and other agencies pursuant to 18 USC 2703(d)

The Defense requests all forensic results and investigative reports by any of the cooperating agencies in this investigation (Department of State (State Department) (DoS) Federal Bureau of Investigation (FBI) Office of the National Counterintelligence (ONCE) Executive (ONCE) Defense Intelligence Agency (DIA) and the Central Intelligence Agency (CIA) (Government Agency))

The Defense should be permitted to argue that by virtue of his expertise and training PFC Manning knew which documents and information could be used to the injury of the United States or to the advantage of any foreign nation. PFC Manning had access to a great deal of very sensitive information that if disclosed could have caused damage to the United States. By selecting the information that he alleged did PFC Manning deliberately choose information that could not cause damage to the United States. The reasonableness of his belief that the information could not cause damage is buttressed by the damage assessments which say that the leaks did not cause damage to the United States

The Defense submits that an expansive reading of "indirectly" as applied in this case renders Article 104 unconstitutionally vague in violation of the Due Process Clause of the Fifth Amendment. If Article 104 is interpreted to reach PFC Manning's alleged conduct it would be constitutionally defective because it would fail to provide sufficient notice of what conduct is prohibited and would fail to provide sufficient guidelines to govern law enforcement

The Defense submits that the damage assessments confirm that PFC Manning did not have "reason to believe" that the information could cause damage to the United States or be used to the advantage of a foreign nation. Further the lack of damage from the leaks supports the view that PFC Manning did not act wantonly or in contempt of the Article 134 offense

The Defense submits that the Government's expansive interpretation of Article 104 renders it substantially over broad in violation of the First Amendment

The Defense submitted its first discovery request on 29 October 2010

The Defense's motion did not contain any classified information A separate attachment to the Defense's motion did not contain any classified information However the Government maintained that by reading these two separate documents together

The Government asked the Investigating Officer Lt. Col. Paul Almazan to find each OCA "not reasonably available for the Article 32 given his position as..."

The Government acknowledged that its argument was made at the behest of the State Department

The intent of the interim order was to ensure no information was published outside of court that included information from discovery via protective order information subject to privilege under MRE 505 and 506 and PII (Personal Identifying Information) to protect witness/participant privacy and safety

The Investigating Officer Lt. Col. Paul Almanza "bending over backwards" to ensure that he could consider such statements despite being proffered in an inadmissible form the Defense should have an opportunity to depose these Original Classification Authority (OCAs). The Government had the full benefit of having its evidence considered by the Investigating Officer but none of the burdens (i.e. cross-examination)

The letter to ODNI (Office of the Director of National Intelligence) from the Assistant General Counsel of the Federal Trade Commission regarding the "documents that were compromised in the Department of State's Net-Centric Diplomacy database" clearly shows that ODNI has conducted some sort of internal review of the cables

The majority of the investigation plan was based on Adrian Lamo of Manning and other documents obtained from Bradley Manning's personnel file

The most glaring example of an abuse of discretion in excluding a period from the R.C.M. 707 speedy trial clock occurred on 4 January 2012 when Lt. Col. Paul Almanza Investigating Officer Article 32 Pretrial purporting to exclude in a one sentence email the days between 23 December 2011 and 3 January 2012 when he did not work on the Article 32 investigation the Defense is aware of no case that contains even a scintilla of support for a "federal holidays and weekends" exclusion or a "time the Government didn't work on the case" exclusion under R.C.M. 707(c) the needless delay in consideration of the Article 13 motion was as always has been the case occasioned by the Government's lack of due diligence

The position of Lt. Paul Almanza Investigating Officer of denying the defense's evidence request is even more indefensible if one considers that representatives of the various government agencies that were investigating the case and/or preparing damage reports were seated in the audience every day at PFC Manning's Article 32 hearing

The reason for this unnatural breakdown of these transactions is obvious the division serves no purpose other than to pile on the charges against PFC Manning in order to increase the likelihood of a severe sentence if he is convicted

THE SPECIFICATION (1): In that Private First Class Bradley E. Manning U.S. Army did at or near Contingency Operating Station Hammer Iraq between on or about 1 November 2009 and on or about 27 May 2010 without proper authority knowingly give intelligence to the enemy through indirect means (UCMJ Article 104)

The term "knowingly" means that the accused had to intend to give the intelligence to the enemy not that the accused knew that by giving it to a third party it might eventually end up in the hands of the enemy

the unnamed officer exercising general court-martial jurisdiction over CW4 James Averhart this case is one of the largest and most complex cases in United States military history

This is supported by the fact that the Investigating Officer Lt. Col. Paul Almanza was completely "wishy-washy" on whether the OCAs would be required to testify. First he determined two days before the Article 32 hearing that the OCAs were not reasonably available. At the hearing he then suggested that the OCAs would be compelled to testify (and thus were reasonably available - at least telephonically). He then reaffirmed that the OCAs were not reasonably available and that he would consider only their unsworn statements

Thomas Smith a counter intelligence agent

Thomas Wheeler President's Intelligence Advisory Board

three (3) military intelligence investigations

Timothy D. Webster

Tiversa Inc. a Federal Bureau of Investigation (FBI) contractor

to the injury of the United States or to the advantage of any foreign nation

Tommy Vietor the National Security Council spokesman

Tony Girmage (sp.) a mentor who with Jason Allen Millman field software engineer contractor at F.O.B. Hammer were the only person assigned to the DCGS-A (Distributed Common Ground Systems)

Touhey Requests

Treasury Secretary Timothy Geithner

Trial Publicity Order

two (2) .csv files each with 100 cables in them in Windows Temp in the allocated space on the Alienware 22

Two unknown redacted individuals who witnessed subsequent reiteration of this order by two unknown individuals whose names were redacted

U.S. Army Computer Crimes Investigation Command (CCICU)

Under the Government's interpretation no criminal intent is required disclosure of information with the mere knowledge that the information disclosed might be accessible to the enemy is punishable under Article 104

UNIDENTIFIED BRIGADE S6

UNIDENTIFIED CAPTAIN former company commander of Headquarters and Headquarters Company (HHC) 2nd Brigade Combat Team (2BCT) 10th Mountain Division (10 MTN Div.) who was replaced by Captain Matthew W. Freeburg around APRIL OR MAY 2010

UNIDENTIFIED CAPTAIN in the S2 SECTION Witness No. 21 of the 2nd Brigade Combat Team 10th Mountain Division

UNIDENTIFIED FEMALE SERGEANT OR SPECIALIST 2ND BRIGADE COMBAT TEAM 10th MOUNTAIN DIVISION

UNIDENTIFIED FEMALE SPECIALIST (No. 1)

UNIDENTIFIED FEMALE SPECIALIST (No. 2)

UNIDENTIFIED FIRST SERGEANT of Headquarters and Headquarters Company 2nd Brigade Combat Team 10th Mountain Division who became 1SG (First Sergeant) in March 2010

UNIDENTIFIED FIRST SERGEANT of Headquarters and Headquarters Company 2nd Brigade Combat Team 10th Mountain Division who became 1SG (First Sergeant) in March 2010 until October 2011

UNIDENTIFIED FIRST SERGEANT of Headquarters and Headquarters Company 2nd Brigade Combat Team 10th Mountain Division who became 1SG (First Sergeant) in March 2010 who CHIEF WARRANT OFFICER FOUR (CW4) AIRSMAN (sp.) recommended take the bolt from PFC Manning's weapon sent him to mental health and then get him out of the Army after December 2009 incident with Sergeant (former Specialist) Daniel Padgett

UNIDENTIFIED INDIVIDUAL Captain Freeburg "sent PFC Manning to an for an evaluation."

UNIDENTIFIED INDIVIDUAL just assumed the position under the approval of the S-2 EITHER MAJOR CLIFF CLAUSEN OR CAPTAIN STEVEN LIM

UNIDENTIFIED INDIVIDUAL who 1st LIEUTENANT ELIZABETH FIELDS she will testify told her "it was an NCO problem and to stay out of it" when she tried to get Pfc Manning help

UNIDENTIFIED INDIVIDUAL who 1st LIEUTENANT ELIZABETH FIELDS thought was a terrible leader because the problems within the unit were constantly being ignored

UNIDENTIFIED INDIVIDUAL who had a conversation with MAJOR CLIFF CLAUSEN about leaving PFC Manning on rear detachment

UNIDENTIFIED INDIVIDUAL who LT COL BRIAN KERNS XO did not believe was not a strong leader [probably Major Cliff Clausen]

UNIDENTIFIED INDIVIDUAL who LT COL BRIAN KERNS XO said command was too generous with and that removing him from his position earlier would have been advantageous

UNIDENTIFIED INDIVIDUAL who Major Cliff Clausen could not provide with accurate or timely estimates or intelligence

UNIDENTIFIED INDIVIDUAL who objected to any changes and would not allow anyone to address the issues surrounding PFC Manning when there was a change in leadership in the S2 section and all of the officers sat down to discuss soldier standards in an attempt to address standard conduct

UNIDENTIFIED INDIVIDUAL who ordered him to take a complete look at INFOSEC across the brigade

UNIDENTIFIED INDIVIDUAL who put out information that Warrant Officers and Noncommissioned Officers were to defer all management responsibilities to defer all management responsibilities to Master Sergeant now Sergeant First Class Adkins

UNIDENTIFIED INDIVIDUAL who told 1ST LIEUTENANT ELIZABETH FIELDS said concerning Pfc. Manning "We need the personnel"

UNIDENTIFIED INDIVIDUAL who told CHIEF WARRANT OFFICER FOUR (CW4) AIRSMAN (sp.) that PFC Manning would deploy due to manpower issues

UNIDENTIFIED INDIVIDUAL who told MAJOR CLIFF CLAUSEN about an outburst by PFC Manning before the deployment

UNIDENTIFIED INDIVIDUAL who was in charge of all enlisted responsibilities

UNIDENTIFIED INDIVIDUAL who told [Captain Freeburg] that PFC Manning's troubles were deeper than the Army could fix and that [Pfc. Manning] should be separated."

UNIDENTIFIED INDIVIDUALS (2) who told CHIEF WARRANT OFFICER FOUR (CW4) he was not responsible for any personnel who worked in the S2 and who CHIEF WARRANT OFFICER FOUR (CW4) went back to for clarification on their expectations about his responsibilities regarding enlisted Soldiers and Officers and his non-role in soldier leadership was reinforced on each occasion

UNIDENTIFIED INDIVIDUALS (2) who an UNIDENTIFIED CAPTAIN IN THE S2 SECTION Witness No. 21 vented to about about how nothing was being done to address PFC Manning's mental and emotional issues

UNIDENTIFIED INDIVIDUALS (2) who did not inform UNIDENTIFIED KEY LEADER OF THE 2ND BRIGADE COMBAT TEAM 10TH MOUNTAIN DIVISION (Art 32 Defense Witness No. 15) gave guidance on who would deploy CMS? Deputy Commander? about Pfc Manning's mental health issues

UNIDENTIFIED INDIVIDUALS (2) who LT COL BRIAN KERNS XO thought were weak leaders (probably Master Sergeant now Sergeant First Class Adkins and Major Cliff Clausen)

UNIDENTIFIED INDIVIDUALS (2) who told UNIDENTIFIED CAPTAIN IN THE S2 SECTION Witness No. 21 to stay in his lane when he tried to address his concerns about Pfc. Manning

UNIDENTIFIED INDIVIDUALS (3) who CHIEF WARRANT OFFICER FOUR (CW4) AIRSMAN (sp.) told that PFC Manning should not deploy

UNIDENTIFIED INDIVIDUALS (3) who CHIEF WARRANT OFFICER FOUR (CW4) AIRSMAN spoke to about his concerns after the outburst in December 2009 by PFC Manning

UNIDENTIFIED INDIVIDUALS (3) who told an UNIDENTIFIED CAPTAIN IN THE S2 SECTION Witness No. 21 to back off when UNIDENTIFIED CAPTAIN IN THE S2 SECTION Witness No. 21 engaged Soldiers on issues as a leader

UNIDENTIFIED KEY LEADER OF THE 2ND BRIGADE COMBAT TEAM 10TH MOUNTAIN DIVISION (Art 32 Defense Witness No. 15) gave guidance on who would deploy CMS? Deputy Commander?

UNIDENTIFIED KEY LEADER OF THE 2ND BRIGADE COMBAT TEAM 10TH MOUNTAIN DIVISION (Art 32 Defense Witness No. 15) provided a sworn statement for the Secretary of the Army's 15-4 investigation into the alleged unauthorized disclosures

UNIDENTIFIED MALE SPECIALIST sworn statement contains an account of Manning translating a document published by Iraq detainees about public corruption which lead to their arrest and how Manning was very upset

UNIDENTIFIED MALE who was the one that worked the security of the T-SCIF and 1ST LIEUTENANT ELIZABETH FIELDS dealt with security clearances this UNIDENTIFIED INDIVIDUAL did not receive any training to be the SSR. However

UNIDENTIFIED MENTAL HEALTH PROFESSIONAL at Behavioral Health that Captain Matthew W. Freeburg went to to discuss PFC Manning's condition

UNIDENTIFIED PRE DEPLOYMENT MENTAL HEALTH who RECOMMENDED THAT MANING NOT DEPLOY

UNIDENTIFIED SGM

UNIDENTIFIED SMG S6 S2 and IO personnel who formed a working group to review Brigade InfoSec

United States Army Counterintelligence Center Cyber Counterintelligence Assessments Branch Department of Defense Intelligence Analysis Program Wikileaks.org - An Online Reference to Foreign Intelligence Services Insurgents Or Terrorist Groups?

United States Army Counterintelligence Center Cyber Counterintelligence Assessments Branch Department of Defense Intelligence Analysis Program's "WikiLeaks.org - An Online Reference to Foreign Intelligence Services Insurgents Or Terrorist Group" as classified at SECRET

United States Forces - Iraq Microsoft Outlook Share Point Exchange Server global address list (GAL)

United States Marshals (US Marshals)

unnamed "mentors" who performed maintenance on the DCGS-A (Distributed Common Ground Systems)

Unnamed agent(s) from US Army CID that took Captain Barclay Keay's sworn statement

unnamed agents four (4) as well as Diplomatic Security Service (DSS) Department of State (State Department) (DoS) interviewed Brady Manning's Aunt Debra Van Alstyne

Unnamed Army CID Agents who accompanied Special Agent Troy Bettencourt on all but one of his interviews of more than 10 unnamed individuals

unnamed Army Criminal Investigation Command (CID) agent who said to Captain Thomas Cherapko when he was concerned about his ability to create forensically sound images "that it was OK because the devices hadn't been seized yet and it's already been so long that they are already tainted"

Unnamed Behavioral Specialist Bradley Manning was taken to after 20 Dec 2009 incident with Sergeant (former Specialist) Daniel Padgett

unnamed civilians seven (7) who Agent Mark Mander Army Computer Crime Investigative Unit (CCIU) says testified were discovered doing "wrong doing" and are being investigated by the Federal Bureau of Investigation (FBI) including in certain aspects the founders owners or managers of WikiLeaks

unnamed commander of Special Agent Toni Graham Army CID who granted her authorization to seize devices

unnamed Commander responsible for DEROGs in the T-SCIF at FOB Hammer Iraq

unnamed commanders at Ft. Belvoir

unnamed Company Commander at Fort Drum NY that was not notified about the early May 2009 incident with Specialist Jihreah Showman and Bradley Manning

unnamed confidential informant

unnamed congressional official who was briefed by the State Department told Reuters "the administration felt compelled to say publicly that the revelations had seriously damaged American interests in order to bolster legal efforts to shut down the WikiLeaks website and bring charges against the leakers"

Unnamed ex co-workers contacted by Army CCIU lead investigation as forensics became available

Unnamed First Sergeant who Sergeant (former Specialist) Daniel Padgett testified that he did not talk to concerning the alleged December 2009 incident with Pfc. Manning. Specialist Jihreah Showman testified that the First Sergeant (WHO IS THIS?) did eventually find out because Showman's commanding officer CW2 (Chief Warrant Officer Two) Hondo Hack told the First Sergeant. Showman testified that Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) did not report the incident to the First Sergeant. Showman testified that she escorted Bradley Manning to meet with the First Sergeant and that she told the First Sergeant that Manning should have never deployed and that this was not the first time and that she was not surprised about the incident

Unnamed Forensic Examiner referred to by Special Agent David Shaver Computer Crimes Investigation Command (CCIU)

Unnamed Government Computer Forensic Experts

Unnamed group of soldiers who Captain Casey Martin (married name is Fulton) spoke to in April 2010 about Collateral Murder

Unnamed individual Adrian Lamo talked to then told two unnamed people (one of the people he told the individual had worked with and the other was a friend - both told law enforcement - one was in the army)

unnamed individual at Department of State (State Department) (DoS) said Intelink after initial Army Computer Crimes Investigation Command (CCIU) attempt to get log files

unnamed individual on Special Agent Toni Graham Army CID team with Thomas Smith a counter intelligence agent

unnamed individual who Adrian Lamo contacted Army Computer Crimes Investigation Command (CCIJ) about and said was chatting with someone else

Unnamed individual who collected Bradley Manning's personal at Camp Arifjan in Kuwait

Unnamed individual who defense asked for the complete contact information for the individual that completed the Classification Review for the item charged in Specification 15 of Charge II: The Defense also requests a copy of the Classification Review for the item charged in Specification 15 of Charge II which is the United States Army Counterintelligence Center Cyber Counterintelligence Assessments Branch Department of Defense Intelligence Analysis Program Wikileaks.org - An Online Reference to Foreign Intelligence Services Insurgents Or Terrorist Groups?

Unnamed individual who reported to David Coombs he was interviewed five or six times

unnamed individual(s) who made "eventually" aware that unnamed soldiers were putting unauthorized software on their computers

Unnamed individual's Captain Steven Lim spoke to in casual conversation about the incident on 20 Dec 2009 with Sergeant (former Specialist) Daniel Padgett

Unnamed individuals in Bradley Manning's Chain of Command

Unnamed individuals in the Forensic Unit of Army Computer Crimes Investigative Unit (CCIJ)

unnamed individuals in the hacker community that Special Agent Antonio Patrick Edwards CCIJ testified Adrian Lamo "knew were involved"

Unnamed individuals interviewed who were military contractors

Unnamed individuals that Captain Barclay Keay asked why soldiers were listening to music and watching movies in the T-SCIF

Unnamed instructors at Fort Huachuca including one whose computer Sergeant First Class Brian Madini's used to view one of three YouTube videos that the same unnamed soldiers had informed him that Bradley Manning had allegedly posted in June 2008 while in training there to become a Fox 35 military intelligence analyst

Unnamed investigating authorities who collected other electronic media other than the hard drives and transferred them sealed to Special Agent Calder Robertson CCIJ

unnamed Lieutenant that Specialist Jihreah Showman testified Bradley Manning was unresponsive to when the Lieutenant asked Bradley Manning was asked to freeze

Unnamed members of Bradley Manning's unit at Fort Huachuca from April to August 2008

unnamed military magistrate that authorized search warrant to search Bradley Manning's personals after he was placed in confinement

unnamed military magistrate who granted Special Agent Toni Graham Army CID a search warrant

unnamed military officers who would request intelligence products to give to the Brigade Commander

unnamed Original Classification Authority (OCA) [probably Ambassador Patrick Kennedy Undersecretary for Management at the Department of State (State Department) (DoS) because defense later filed a Touthy request for him after this motion was ruled on] informed the Government of "a possible Touthy issue"

unnamed Original Classification Authority (OCA) defense learned about after 2 December 2012

Unnamed people on Special Agent Calder Robertson CCIJ team who instructed Captain Thomas Cherepko on how to obtain server logs from the network and shared drive as well as email logs and how to conduct forensic analysis

unnamed person at headquarters who called Special Agent Toni Graham Army CID

unnamed person whom Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) reported an incident where Specialist Jihreah Showman counseled Bradley Manning about completely his tasks where Showman said Manning allegedly told her that he wasn't getting task complete was because of his paranoia of others

unnamed Quantico watch supervisor on the nightshift of 13 March 2011

unnamed redacted forensic psychiatrist at Quantico Brig that said "You know Sir I am concerned because if you are going to do that maybe you want to call it something else because it is not based upon anything from behavioral health" and "Well then don't say it is based upon mental health You can say it is Maximum Custody and just don't put that we [behavioral health] are somehow involved in this"

unnamed S2 at the T-SCIF at FOB Hammer Iraq

unnamed S2 that Master Sergeant Paul David Adkins (now Sergeant 1st Class due to administrative action) informed about the early May 2009 incident with Specialist Jihreah Showman and Bradley Manning at Fort Drum NY

Unnamed Signal Intelligence Analysts

unnamed soldier and unnamed three (3) or four (4) officers who were watching Jul 2007 Baghdad Apache airstrike video known in the T-SCIF with Specialist Jihreah Showman before it was leaked and published by WikiLeaks as Collateral Murder

unnamed soldiers in the Supply Room at FOB Hammer Iraq

Unnamed soldiers in the T-SCIF who bought pirated movies from Iraqis and play on their D6 machines

unnamed soldiers in the T-SCIF who Jason Alan Millan a field software engineer contractor saw had programs installed on their DCGS-A (Distributed Common Ground Systems)

Unnamed soldiers in the T-SCIF who would pull music from the shared drive and put it on their D6 Computers

unnamed soldiers in the T-SCIF who would pull music from the shared drive and put it on their D6 Computers

Unnamed soldiers who Captain Barclay Keay testified he saw listening to music of watching movies in the T-SCIF at FOB Hammer

unnamed soldiers who saw Bradley Manning running around at night and joked about it

unnamed soldiers who would play games on their D6 Computers

unnamed Special Agent Army Computer Crimes Investigation Command (CCIJ) who did analysis of media from Iraq with Special Agent Schaller Army Computer Crimes Investigation Command (CCIJ) and Special Agent Johnson Army Computer Crimes Investigation Command (CCIJ)

unnamed Specialist who replaced Specialist Jihreah Showman as NCOIC of the night-shift at the T-SCIF at FOB Hammer Iraq

Unnamed supervisors whom Captain Thomas Cherepko notified about unauthorized music and games on the shared SIPRNet T-Dive

unnamed Supply Room clerk at FOB Hammer Iraq

Unnamed two (2) Army Computer Crime Investigative Unit (CCIJ) agents sent to CENTCOM second week of June in Florida where they obtained log files related to investigation of the Garam airstrike video

unnamed two (2) NCO [Non Commissioned Officers] escorted Manning into custody

US Army Intelligence (G-2)

US complicity in torture and public corruption in Iraq

Vice Admiral Robert S. Harward Deputy Commander US Central Command CENTCOM the Original Classification Authority for the classification determination and impact on national security for the CIDNE Afghanistan Events [Afghan War Diary] CIDNE Iraq Events [Iraq War Logs] other briefings and the BE22PAX.wmv video [Garam Airstrike Video]

Vice President Joseph Biden

Video of Manning Quantico Interrogation and Stripping on January 18

Warning Banner

Warrant Officer One (WO1) Kyle Balioneck

We still haven't heard yet of ODNI (Office of the Director of National Intelligence) has a damage assessment

Wget

where Coombs identified Cully (sp. as a civilian)

Whether the accused in fact knew or had a reason to believe the charged information could be used to the injury of the United States or to the advantage of any foreign nation is not determined by the OCA

While the Government may prefer that those who come under the aim of its prosecutorial crosshairs go quietly into the night the United States Constitution permits a defendant to do otherwise a) Maintaining that Brady does not require the Government to turn over documents that are relevant to punishment b) Maintaining that R.C.M. 703 does not apply to classified discovery c) Disputing the relevance of facially relevant items (such as damage assessments) d) Using the R.C.M. 703 standard instead of the appropriate R.C.M. 701 standard when dealing with items within the military's possession custody and control e) Referring to damage assessments and other documents as "alleged" to frustrate the Defense's access to them f) Maintaining that the Department of State (State Department) (DoS) and ONIC had not "completed" a damage assessment g) Maintaining that it was "unaware" of forensic results and investigative files h) Resisting production of the Department of State (State Department) (DoS) damage assessment under the "authority" of *Giles v. Maryland* 388 U.S. 66 117 (1967) (which provided no legal support for its position) i) Despite understanding Defense discovery requests defining "damage assessments" and "investigations" to avoid producing discovery. After instructing the Defense that it should not use the term "damage assessments" to refer to informal reviews of harm (instead to use "working papers") then referring to working papers as "damage assessments" j) Insisting on a threshold of specificity for Brady requests that does not exist or some additional showing of relevance k) Maintaining that the FBI investigative file was not material to the preparation of the defense to which the Court quizzically asked "How could the investigative file not be material to the preparation of the defense?" l) Maintaining that anything that predated the Department of State (State Department) (DoS) Damage assessment was not discoverable because it was "likely" cumulative m) Arguing with the Court at length about whether the Government was obligated to turn over documents that were obviously material to the preparation of the defense absent a "specific request" n) Waiting until two days before the Defense's Article 13 filing before reviewing 1374 emails from Quantic which it had in its possession for over six months

While the OCA's determinations were at one point in history "worthy of great deference" such is not necessarily the case anymore. The United States has acknowledged that it has a problem with who was on the prosecution's original witness list dated July 7

who was on the prosecution's original witness list dated July 7

Why is the Government arbitrarily drawing the line at the grand jury testimony? Why is the grand jury testimony not in the Government's possession custody and control when the other FBI files are?

WikiLeaks

WikiLeaks and/or the damage occasioned by the alleged leaks

WikiLeaks Mitigation Team at the Department of State (State Department) (DoS)

WikiLeaks Most Wanted List

WikiLeaks.org Twitter Account

WikiLeaks.org Web Archive

Williams

Wired.com

what "in large part be hearsay evidence about what other agents have done on the case and what witnesses have told these other case agents"

yada tar.bz2.nc made on January 30 2010 at 10:22 p.m in the allocated space of an SD card allegedly obtained at the second search of Debra Van Alstyne Bradley Manning's aunt home after having allegedly been shipped from Iraq in October 2010 Four (4) files contained in yada tar.bz2.nc. They were: Screenshot of `afg_events.csv` dated 8 January 10. Government said contained 91000 individual CIDRE reports for Afghanistan Screenshot of `iraq_events.csv` dated 5 January 2010. Government said contained 400000 individual reports that are CIDRE reports from Iraq Screenshot of README dated 9 January 2010. Government said was a temporary file created by Macintosh OS Screenshot of `_README.TXT` dated 9 January 2010 Government said the last of this document said "This is possibly one of the more significant document of our time removing the fog of war revealing the true nature of 21st century asymmetric warfare. Have a good day." The note also specifically stated that steps had been taken to sanitize certain sensitive data and that there should be a 90 to 100 day wait before releasing data to best assess how to distribute the information and protect the source. Two encrypted files [not clear if allocated or unallocated] both of which were unrecoverable and both of which allegedly referenced the word "nathan" in the title i.e. `"nathan2_events_tar_bz2"` Document 1: Screen shot of [Missed] `Manningb_006507` [Missed] that Government asked Shaver to authenticate Document 2: Email from Manning's Thunderbird account that Government asked Shaver to authenticate Document 3: 8 April 2010 email from Manning's Thunderbird account that Government asked Shaver to authenticate `Manningb_00409656` Document 4: 10 April 2010 Email from Manning's Thunderbird account that Government asked Shaver to authenticate

Archives

aixxaorien.com | blog | interviews | audio | video | features | about | in the press | contact | archives | time line | redacted names and notables



This work by Aixxa O'Brien is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License. Permissions beyond the scope of this license may be available at email@aixxaorien.com.

UNCLASSIFIED

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)

PFC, U.S. Army,)

HHC, U.S. Army Garrison,)

Joint Base Myer-Henderson Hall)

Fort Myer, Virginia 22211)

Prosecution Objection to
Providing an "Example" Witness
to Examine the Viability of
Reasonable Alternatives to Closure

Enclosure 7

3 April 2013

UNCLASSIFIED

Encl 7 to
APPELLATE EXHIBIT 512
PAGE REFERENCED: _____
PAGE ____ OF ____ PAGES

alexobrien.com | blog | interviews | audio | video | features | about | in the press | contact | archives | time line | redacted names and notables

Results tagged "REDACTED Commander's WHAT IS THIS?"

Witness | US v Pfc. Manning, Lt. Col. Brian Kerns, Executive Officer (XO), 2nd Brigade Combat Team, 10th Mountain Division

by Alexa O'Brien on December 8, 2011 11:55 AM

US v. Pfc. Bradley Manning is being conducted in *de facto* secrecy. This page is a work in progress and may contain errors. The page is developing and may be updated. All updates and amendments will be noted.

For more information on the lack of public and press access to United States v. Pfc. Bradley Manning, visit the *Center for Constitutional Rights*, which filed a petition requesting the Army Court of Criminal Appeals (ACCA) to order the Judge to grant the public and press access to the government's motion papers, the courts own orders, and transcripts of proceedings, none of which have been made public to date."



Lt. Col. Brian Kerns was the Executive Officer (XO) for the 2nd Brigade Combat Team, 10th Mountain Division, and the second most senior commanding officer in Pfc. Manning's chain of command within the 2nd Brigade Combat Team, 10th Mountain Division.

Lt. Col. Brian Kerns, Executive Officer (XO), 2nd Brigade Combat Team, 10th Mountain Division provided a sworn statement for the Secretary of the Army's 15-6 investigation into the alleged unauthorized disclosures.

The Government objected to the defense request for the testimony of Lt. Col. Brian Kerns, Executive Officer (XO), 2nd Brigade Combat Team, 10th Mountain Division on December 1, 2011 Article 32 Pretrial Hearing, stating his testimony was "not relevant to the Article 32 investigation and will only serve to distract from the relevant issues." While there is no official public record of Alimenza's denial of this witness' testimony, Lt. Col. Brian Kerns, Executive Officer (XO), 2nd Brigade Combat Team, 10th Mountain Division did not appear during any open session of the Article 32 Pretrial Hearing. The public record shows that at least fourteen witnesses were called to defense for the Article 32 Pretrial Hearing. In Lt. Col. Alimenza's ruling on the Defense Request for Article 32 Witnesses, 12 witnesses were granted to the defense, 10 of whom were also requested by the Government. Defense said in open Court on December 16, 2011, that Lt. Col. Alimenza granted two additional witnesses to defense that morning.

The defense's account of Lt. Col. Brian Kerns, Executive Officer (XO), 2nd Brigade Combat Team, 10th Mountain Division sworn statement is contained in Defense Request for Article 32 Witnesses

No. 14 on the December 2, 2011 Defense Request for Article 32 Witnesses

[Lt. Col. Brian Kerns, Executive Officer (XO), 2nd Brigade Combat Team, 10th Mountain Division] He will testify that he was [redacted] [Maj. Cliff Clausen, Brigade S2] direct supervisor. He believed that [redacted] [Maj. Cliff Clausen, Brigade S2] could not provide [redacted] WHO IS THIS? with accurate or timely estimates or intelligence, and could not talk to [redacted] [Col. David M. Miller, Commander of the 10th Mountain Division's Second Brigade] in a way that served the Commander's [WHAT IS THIS?] needs. The brigade commander [Col. David M. Miller, commander of the 10th Mountain Division's Second Brigade] finally lost confidence in [redacted] [Major Cliff Clausen, Brigade S2] and made the decision after approximately 6 months not to move him. He will testify that the unit did not conduct a formal relief for cause, but moved him to a transition team. According to [redacted] [Lt. Col. Brian Kerns], [redacted] [Major Cliff Clausen, Brigade S2] performance was weak, but not so weak as to warrant a relief for cause [redacted] [Lt. Col. Brian Kerns] did not believe [redacted] [Major Cliff Clausen, Brigade S2] was not a strong leader. He tried to decentralize operations but didn't have enough oversight to control. He empowered junior members who were too inexperienced to do the job and did not step in to correct when they made mistakes. He will testify that [redacted] [Maj. Cliff Clausen, Brigade S2] was unable to mentor or develop younger officers and didn't have much direct control over the shop. He will also testify that [redacted] [Maj. Cliff Clausen, Brigade S2] was handicapped by weak NCO [Non-commissioned Officer] leadership in his shop. Specifically, his NCOG [Non-commissioned Officer in Charge], then [redacted] [Master Sergeant Paul David Adkins (now Sergeant First Class due to administrative actions)] was not an effective leader. In his opinion, both [redacted] WHO IS THIS? and [redacted] WHO IS THIS? were weak leaders. He will testify that he was unaware of any leadership guidance provided in the S2 sections regarding enlisted personnel management. He will testify that it did not surprise him that [redacted] WHO IS THIS? put out information that Warrent Officers and Non-commissioned Officers were to offer all management responsibilities to [redacted] Master Sergeant Paul David Adkins (now Sergeant First Class due to administrative actions). He will testify that perhaps the command was too generous with [redacted] WHO IS THIS? and that removing him from his position earlier would have been advantageous. He will testify that he believes PFC Manning's mental and emotional issues were more than enough to put others at risk and should have resulted in an immediate DEROG. He will testify that he did not know anything about PFC Manning's conduct until a recommendation for separation was made by the chain of command. He will testify that none of the mental or emotional health concerns, prior to May of 2010, made it to his level. [Lt. Col. Brian Kerns] will testify that the failure to properly DEROG PFC Manning's was the unit's biggest failure. He believes that the unit should have pulled PFC Manning's access to classified information much earlier. He will testify that the unit should have recognized him as needing help and that his condition made him unfit for service as an intelligence analyst. He will also testify that the assistant S6 for the brigade [redacted] CPT Thomas Chervick) came to him with concerns about unauthorized personal media on SIPRNet machines. According to [redacted] CPT Thomas Chervick, [redacted] [Lt. Col. Brian Kerns] will testify that it was fairly common for the unit to send to see games, music and movies on the SIPRNet. He believed that it was very common to see [redacted] [Lt. Col. Brian Kerns] will testify that the staff to do the right thing, but he didn't want to be the standard. He will testify that at no point was UCMJ punishment applied to those who were placing unauthorized information on SIPRNet. He will acknowledge that with respect to the media on the SIPRNet, he believed that the Army had become too comfortable working on SIPRNet while deployed. It is his opinion that this may have bred some complacency because of the ease of access. He believes that most Soldiers did not realize that placing music and other media on SIPRNet computers was wrong because of how prevalent those items were across Iraq. He will also testify that after PFC Manning was arrested, [redacted] WHO IS THIS? ordered him to isolate his computer and to stop putting unauthorized media on computers such as investigations (1) consisting of the SGM (UNIDENTIFIED SERGEANT MAJOR) S2 (Captain Steven Lin, then Assistant S2 and Military Intelligence Company Commander), S6 (UNIDENTIFIED S6) and IO (Information Operations) (UNIDENTIFIED INFORMATION OPERATIONS) personnel to look at how the brigade was operating. Based upon this review, the S6 (UNIDENTIFIED S6) removed universal ability to write to disks; there was additional compartmentalizing of information within the BCT based on a need to know; the S6 (UNIDENTIFIED S6) instructed staff on how to lock out directories and the brigade established an SOP on the implementation for reviewing infractions for potential DEROG actions

Other Resources

- Fox, Lt. Colonel Brian Kerns, "Iraq Security 'Phenomenally' Improved" (Video)
- Defense Request for Article 32 Witnesses



Alexa O'Brien
carwinb

kenethbipg Email to Attorney Jason Flores-Williams regarding the Motion to Quash Prosecutor's Subpoena to Oxouffare b6Ly/14NCVZ 7 hours ago reply selected favorite

carwinb @enquerre Tr 32 minutes ago reply selected favorite

enquerre Audio of @JulianBurnside speaking last night in @Abilene at a #swedjude event vimeo.com/63258441 cc: @m_cetera @carwinb @twikileaks 34 minutes ago reply selected favorite

carwinb In the end the US cannot give us class 1 yet 11 hours ago reply selected favorite

Join the conversation

Categories

- Features (16)
- GTMO (14)
- Idea (13)
- In the Press (52)
- Interviews with... (36)
- NDAAs, Hedges et al v Obama et al (13)
- Occupy Wall Street (62)
- Panel Discussions (7)
- Podcast Video (1)
- Podcasts Audio (16)
- Published on WJ, Control (2)
- Regions or Countries
- Bahrain (6)
- Balkans (1)
- Cambodia (1)
- Egypt (3)
- Europe (2)
- Gaza (2)
- Iran (6)
- Saudi Arabia (1)
- Yemen (1)
- View on Twitter
- Whistleblower Protection Act (3)
- WikiLeaks (43)
- Bradley Manning (34)
- Chain of Command (10)
- Donate (1)
- Interviews (4)
- Investigations (1)
- Central Intelligence Agency
- Department of Defense (1)
- Secretary of the Army 15-6 (1)
- Department of Justice
- Federal Bureau of Investigation
- Department of State
- US v. Pfc. Manning Update (2)
- US v. Pfc. Manning Aspinette Exhibits (11)
- US v. Pfc. Manning Charges (4)
- US v. Pfc. Manning Damage Assessments (3)
- State Department (1)
- US v. Pfc. Manning Defense (1)
- US v. Pfc. Manning Legal Filings (51)
- 10 USC 904 aiding the enemy (4)
- 18 USC 1030 exceed authorized access (6)

• Defense Request to Compel the Production of Article 32 Witnesses

1

18 USC 2703d (1)
16 USC 641 Public money property or records (2)
18 USC 793 espionage (3)
Article 13 (8)
Discovery (20)
Harm (2)
Lesser Included Offenses (3)
Plea and Forum (7)
Protective Order (1)
Speedy Trial (1)
Witness Lists (8)
U.S. v. Pfc. Manning Military District of Washington (2)
U.S. v. Pfc. Manning Officials of the Court (3)
U.S. v. Pfc. Manning Prosecutors (1)
U.S. v. Pfc. Manning Transcripts (28)
U.S. v. Pfc. Manning Witness Profiles (60)
Agents (11)
Informants (1)
Original Classification Authorities (OCAs) (7)
Pretrial Confinement (13)
US Army (29)
White House (1)
Sweden v. Assange (1)
U.S. v. WikiLeaks Investigating US Agents and Officials (5)
U.S. v. WikiLeaks Time Line (2)
WikiLeaks Grand Jury (11)
WikiLeaks Grand Jury Legal Dockets and Files (8)
16 USC 2703d (1)
WikiLeaks Grand Jury Prosecutors (3)
WikiLeaks Grand Jury Witness Profiles (2)
usdayofrage.org (59)

☐ Subscribe☐ Feed of results tagged "REDACTED Commander's WHAT IS THIS?" needs

[alexaobrien.com](#) | [blog](#) | [interviews](#) | [audio](#) | [video](#) | [features](#) | [about](#) | [in the press](#) | [contact](#) | [archives](#) | [time line](#) | [redacted names and notables](#)



This work by Alexa O'Brien is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License
Permissions beyond the scope of this license may be available at email@alexaobrien.com

FOR OFFICIAL USE ONLY

PUBLIC AFFAIRS (CCPA)				
Information revealing	Classification	Declassification	Reason	Remarks
Public affairs contingency statement	U	N/A	N/A	

FOR OFFICIAL USE ONLY

PROVOST MARSHAL (JSD)				
Information revealing	Classification	Declassification	Reason	Remarks
Deployment / redeployment of security augmentation troops when combined with dates and/or locations	U	N/A	1.4(a) / 1.4(g)	Classified only during periods of increased threat; included are numbers of personnel, dates, and locations.
Enemy prisoner of war (EPW) information that reveals locations of units or EPW camps; unit strength and/or military capabilities; or number of EPWs	S	Upon completion of operation/ hostilities	1.4(a) / 1.4(c) / 1.4(g)	
Physical security vulnerabilities and vulnerability to terrorist attack	S	Upon correction or after 5 years if uncorrected	1.4(g)	
Threat condition	U	N/A	N/A	
Detailed terrorist threat level/condition	C	10 years	1.4(a) / 1.4(g)	May be classified higher upon direction of an OCA
General terrorist threat information	U	N/A	N/A	All terrorist threat information must contain unclassified tear line for widest dissemination

FOR OFFICIAL USE ONLY

FORCE PROTECTION (JSD) Cont.				
Information revealing	Classification	Declassification	Reason	Remarks
Vulnerability assessments and trends	S	10 years	1.4(g)	May be declassified upon resolution of all vulnerabilities without a waiver
Purchase request package	U	N/A	N/A	For Official Use Only
Electronic Sweeps				
General information not revealing any details	C	10 years		See AFI 71-19 for strict need-to-know guidance
Specific information revealing date range and area to be swept	S	10 years		
Target area weather information	S	10 years or upon plan execution, if executed	1.4(a)	
Top secret options; discussion of	TS	10 years	1.4(a)	

FOR OFFICIAL USE ONLY



Attack the Network – Defeat the Device – Train the Force

SECURITY CLASSIFICATION GUIDE

for

JOINT IMPROVISED EXPLOSIVE DEVICE DEFEAT ORGANIZATION (JIEDDO)

DISTRIBUTION STATEMENT D: Distribution authorized to the Department of Defense and U.S. DoD contractors only, administrative or operational use, effective the approval date of this document. Other requests for this document shall be referred to the JIEDDO Security Office.

This document contains information
EXEMPT FROM MANDATORY DISCLOSURE
Under the Freedom Of Information Act (FOIA).
Exemption 2 applies.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Security Classification Guide

for

Joint Improvised Explosive Device Defeat Organization (JIEDDO)

Date: _____

Approved By: _____

Michael D. Barbero, LTG
Director
Joint IED Defeat Organization

Issued By: Joint IED Defeat Organization
5000 Army Pentagon
Washington, DC 20310-5000

Action Officer: Mr. John E. Nimitz
Security Officer/SSR
Joint IED Defeat Organization
703-601-4744

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

1. PURPOSE

This Security Classification Guide (SCG) is a living document that provides guidance and instructions on the classification, marking and distribution of information involved in the development and eventual employment of tactics, techniques, procedures (TTP) and technologies that enable the Joint Improvised Explosive Device Defeat (IED) Organization (JIEDDO) to defeat the IED threat. This SCG addresses security measures to safeguard developmental efforts within the organization as well as already developed end items that require ongoing protection measures. As the organization matures, JIEDDO will update the SCG to address additional IED defeat developmental efforts requiring protection. Future revisions to this SCG will update declassification dates in light of fielding dates and other program milestones, as well as technology commercialization and/or obsolescence. Any suggested changes or updates to this SCG will be provided in writing to the Office of Primary Responsibility (OPR) as indicated in paragraph three.

2. AUTHORITY

This SCG is issued under authority of Executive Order (E.O.) 12958, as amended 25 March 2003, and DoDI 5200.1-R (Information Security Program). This SCG constitutes authority and may be cited as the basis for classification, downgrading, or declassification of material related to the JIEDDO activities in support of DoD Directive 2000.19E, Joint Improvised Explosive Device Defeat. Unless otherwise noted, information or material identified as CLASSIFIED by this SCG is classified by authority of the JIEDDO Original Classification Authority identified on the title page.

3. OFFICE OF PRIMARY RESPONSIBILITY (OPR)

This SCG is issued by and all inquiries for information concerning its content should be addressed to the Joint Improvised Explosive Device Defeat Organization (JIEDDO), Attn: Director, 5000 Army Pentagon, Washington DC 20310-5000.

4. CLASSIFICATION CHALLENGES

Questions concerning the content and interpretation of this SCG should be directed to the issuing activity. If the security classification imposed by this SCG is considered impractical, documented and justified recommendations should be made through appropriate channels to the issuing activity. If current conditions, progress made in this effort, scientific or technological developments, advances in the state-of-the-art or other factors indicate a need for changes, similar recommendations should be made. Pending a final decision, the information involved will be protected at either the currently specified level or the recommended level, whichever is higher. All users of this SCG are encouraged to assist in improving its currency and adequacy. Any classification challenges should be brought to the attention of the OPR.

FOR OFFICIAL USE ONLY

5. REPRODUCTION, EXTRACTION AND DISSEMINATION

Copies of this SCG and all extracts thereof will be made, stored, and transmitted in accordance with (IAW) authorized procedures corresponding to the classification of the information involved. Authorized recipients of this SCG may reproduce, extract, and disseminate the contents of this SCG, as necessary, for use by specified groups, including industrial activities that are involved in IED Defeat development, test, or operations.

6. PUBLIC RELEASE

The fact that this SCG contains certain details of unclassified information does not permit automatic public release of the information. Proposed public disclosures of the JIEDDO's unclassified information regarding the technologies and activities shall be processed through appropriate channels for approval to publish. Requests for public release certification must be submitted in accordance with DoD Directive 5230.9 (Clearance of DoD Information for Public Release), DoD Regulation 5400.7 (DoD Freedom of Information Act Program), and the Industrial Security Manual for Safeguarding Classified Information (Section 5 Disclosure). Defense contractors, military members as well as government service employees shall comply with DoD Manual 5220.22-M (National Industrial Security Program Operational Manual (NISPOM)) and other requirements that may be directed by the Government.

Only information that has been reviewed and certified for public release may be released. However, the decision or authority to release information belongs to the Public Affairs office. The OPR will process requests for approval as outlined below.

Any proposed release to the public of official information pertaining to the JIEDDO must be forwarded to the JIEDDO, STRATCOM for review and further processing. The term "release" applies, but is not limited to, articles, speeches, briefs, papers, photographs, brochures, advertisements, displays, presentations, etc., on any JIEDDO related activity. It is incumbent upon defense contractors, or other agencies, to screen all information submitted by them for the material certification to ensure that it is both unclassified and technically accurate. Letters of transmittal shall contain certification to this effect. The number of copies produced, and distribution of the document, must be strictly controlled until review is completed. If suspected classified information is found during the review process, all holders of the document will be informed of the degree of protection required. When doubt exists concerning the classified status of a proposed release pertaining to the JIEDDO, Security will render the final decision. The material submitted for review must include a valid suspense date, if applicable. Requests for public release certification, according to DoD Manual 5220.22-M, NISPOM (attachment to DD Form 441, Security Agreement), must be submitted to the JIEDDO, STRATCOM for review and further processing. Electronic copies (unless submitted via Secret Internet Protocol Router Network (SIPRNet)) of the proposed public release material must be submitted to JIEDDO, STRATCOM at least two weeks before approval is needed.

FOR OFFICIAL USE ONLY

Approval for public release does not necessarily satisfy export-licensing requirements of the Departments of State and Commerce. Export-controlled material will not be entered into the security review channels for public release approval to circumvent the licensing requirements of the Departments of State and Commerce.

Release of Program Data on the World Wide Web: Extreme care must be taken when considering information for release onto publicly accessible or unprotected World Wide Web sites. In addition to satisfying all of the aforementioned approval provisions, owners and/or releasers of information proposed for such release must ensure that it is not susceptible to compilation with other information to render sensitive or even classified data in the aggregate. The search and data mining capabilities of Web technology must be assessed from a risk management perspective. If there are any doubts, do not release the information!

Release of information to foreign government service employees, international organizations and/or their representatives: Any military activity or defense contractor receiving a request for, or proposing to release information on this program will forward such requests/proposals to the OPR, after compliance with the following:

- Military activities will comply with the National Policy and Procedure for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1).
- Defense contractors will comply with the Department of State International Traffic in Arms Regulation (ITAR).

NOTE: Foreign national employees of the contractor or sub-contractor, including those possessing reciprocal clearances, are not authorized access to classified information resulting from or used in the performance of their contract unless authorized in writing by the OPR. Contractors shall ensure that this SCG, including all applicable standard security precautions and regulations identified in their DD Form 254, Contract Security Requirement, are complied with. Prime contractors are responsible for ensuring each of their subcontractors are aware of, and comply with, these requirements. Material proposed for release by subcontractors will be routed through their prime contractor.

Release of information to the United States Agencies: Requests will be submitted to the OPR.

Release of information at symposia, seminars, and conferences: Requests for such releases of classified information shall be submitted to the OPR for review and approval. Material will be submitted a minimum of six weeks prior to proposed release date in electronic format. Any information authorized for release will reflect that the work reported upon is sponsored by the DoD. If foreign nationals are expected to be present at such a conference, the provisions of paragraph 7 below must be followed.

FOR OFFICIAL USE ONLY

Use of information or data classified by a foreign government: If information or data has been previously classified by a foreign government, this information or data will be classified at a level which will accord at least the same degree of protection as provided by the foreign government classification. This procedure will be adhered to even though a higher classification than that normally imposed by the U.S. for the same type of information will result.

7. FOREIGN DISCLOSURE

Foreign disclosure is the sharing of US classified information with foreign governments or international organizations in support of established or approved planned international programs. Any disclosure to foreign officials of information classified by this SCG shall be in accordance with the procedures set forth in DoD Directive (DoDD) 5230.11, DoDI 5230.27 and National Disclosure Policy (NDP-1). A foreign disclosure review shall be conducted prior to issuance of any solicitation. This review should result in a determination regarding which foreign governments and international organizations (and their industrial entities) will be permitted to participate in the solicitation.

General Release Guidance: Classified information is only released to properly cleared persons on a need-to-know basis and through government-to-government channels. It is the responsibility of the individual actually releasing the information to verify that the recipient is a foreign official authorized to receive classified information on behalf of his/her government or international organization and that information has been properly approved for release. JIEDDO personnel originating material classified by this guide will mark it as it is created in accordance with DoDI 5200.1-R, "Information Security Program," January 1997. JIEDDO information developed within combined spaces is presumed to be releasable to foreign nations represented in those spaces and should be marked "[CLASSIFICATION]/REL TO USA, [COUNTRY OR ORGANIZATION CODE]." When information is derived from multiple sources, the most restrictive handling and declassification instructions apply to the derived document. Classified information not explicitly marked releasable to a particular country shall not be released without proper authorization from the originating Foreign Disclosure Officer.

According to DoDD 5230.11, under conditions of actual or imminent hostilities such as Operation Iraqi Freedom or Operation Enduring Freedom, any unified or specified commander may disclose classified military information (CMI) through TOP SECRET to an actively participating allied force when support of combined combat operations requires the disclosure of that information. Under such circumstances, the Chairman, National Disclosure Policy Committee will issue further guidance determining any limitations that should be imposed on continuing disclosure of that information. When an authorized disclosure official (such as a Foreign Disclosure Officer (FDO)) has made a determination that CMI originated by JIEDDO is releasable under these conditions, the FDO should mark that information "[CLASSIFICATION]/REL TO USA, [COUNTRY OR ORGANIZATION CODE]," and forward an information copy to the JIEDDO FDO. A foreign disclosure review shall be conducted prior to issuance of any solicitation. This review should result in a determination regarding their foreign governments and

FOR OFFICIAL USE ONLY

international organizations (and their industrial entities) permitted to participate in the solicitation.

8. FOREIGN GOVERNMENT INFORMATION AND FOREIGN MILITARY SALES

U.S. government information is furnished upon the condition that it will not be released to other nations without specific authority of the DoD of the United States. Subject release of information provides that individual or corporate rights originating the information will be provided substantially the same degree of security afforded it by the Department of Defense of the United States.

9. FOR OFFICIAL USE ONLY (FOUO) CAVEAT

For Official Use Only (FOUO) is not a security classification. FOUO information has not been given a security classification pursuant to the criteria in this SCG, but may be withheld from the public for one or more of the reasons cited in EO 12958, as amended, and DoDI 5200.1-R. Information so designated in this SCG that warrants FOUO markings will be handled and protected in accordance with regulations. The SCG for Freedom Of Information Act (FOIA) markings is intended solely as a guide. One, none or all of the suggested FOIA exemptions may apply to particular information depending on the particular facts of the information being protected or disclosed.

This document contains information EXEMPT
FROM MANDATORY DISCLOSURE under the
FOIA. Exemption(s) ... apply/applies.

ALL Freedom of Information Act (FOIA) exemptions identified in this SCG:

Number 1. Material appropriately classified by this SCG is similarly exempt from disclosure as National Security Information under FOIA.

Number 2. Related solely to the internal personnel rules and practices of the DoD or any of its components. Records containing or constituting statutes, rules, regulations, orders, manuals, directives, instructions, and security classification guides. This classification encompasses "High 2" information (i.e., information that would allow persons to circumvent or undermine JIEDDO's internal practices) and "Low 2" information (i.e., information of a trivial administrative nature.)

Number 3. Records protected by another law that specifically exempts the information from public release. Applicable to technical Controlled Unclassified Information (CUI).

Number 4. Containing trade secrets or commercial or financial information that a DoD Component receives from a person or organization outside the Government which is likely to cause substantial harm to the competitive position of the source, impair the Government's ability to obtain necessary information in the future, or impair some other

FOR OFFICIAL USE ONLY

legitimate Government interest. Some examples: Commercial or financial information received in confidence in connection with bids, contracts, or proposals; statistical data and commercial or financial information concerning contract performance, income, etc.; personal statements given in the course of inspections, investigations, or audits; financial data provided in confidence by private employers in connection with locality wage surveys; scientific and manufacturing processes or developments concerning technical or scientific data or other information submitted with an application for a grant or with a report while research is in progress; technical or scientific data developed by a contractor or subcontractor exclusively at private expense and technical or scientific data developed in part with federal funds and in part at private expense; computer software which is copyrighted; or, proprietary information submitted strictly on a voluntary basis.

Number 5. Subjective evaluations that are reflected in records pertaining to the decision-making process of an agency. Examples are: advice, suggestions or evaluations prepared on behalf of the DoD; non-factual portions of evaluations by DoD component personnel of contractors and their products; information of a speculative, tentative or evaluative nature; trade secret or other confidential research development; and portions of official reports on inspection, reports of the IG, audits, investigations, or surveys pertaining to safety, security, or the internal management, administration or operation of one or more DoD components.

10. DISTRIBUTION STATEMENT

Distribution statements are required to be placed on all technical documents no matter if they are classified or unclassified. Export controlled warning notices will be applied only to technical documents containing critical technology. These notices will be placed on the front cover or first page of the document. When possible, parts that contain information creating the requirement for a distribution statement or other warning notice shall be prepared as an appendix to permit broader distribution of the basic document.

Technical documents contain information (experimental, developmental, engineering works) that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul material. The information may be in text, graphic, or pictorial form.

The following statements will be applied to all technical documents as defined as above:

DISTRIBUTION STATEMENT D: Distribution authorized to the Department of Defense and U.S. DoD contractors (fill in reason) (date of determination). Other requests for this document shall be referred to the JIEDDO Security Office.
--

Reasons for applying distribution D:

FOR OFFICIAL USE ONLY

Foreign Government Information: To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information.

Administrative or Operational Use: To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.

Software Documentation: Releasable only in accordance with DoD Instruction 7930.2, Automatic Data Processing (ADP) software exchange and release.

Transfer of data from SIPR to a CD: Transfer of data from SIPR to a CD: Any data that needs to be transferred from SIPR to a CD must be done in accordance with US CYPERCOM CTO 10-133. Currently J6 and STRATCOM are the only authorized divisions that transfer data. All CD with SIPR Data or higher must bear the proper security marks (AR 380-5). Any CD(s) that needs to be mailed/hand carried out of the Polk building must go through JIEDDO Security. For further guidance, please contact JIEDDO Security.

Critical Technology: To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of DoDD 5230.25. Apply the following notice to the front cover or title page:

Warning - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, USC, Sec 2751 etc) or the Export Administration Act of 1979, as amended (Title 50, USC, App 2401 etc). Violations of these export laws are subject to severe criminal penalties.

Specific Authority: To protect information not specifically included in the above reasons and discussions, but which requires protection in accordance with valid documented authority such as executive orders, classification guides, DoD or DoD component regulatory documents. When filling in the reasons, cite "Specific Authority (identification of valid documented authority)."

At times, the application of a different distribution statement may be necessary to facilitate sharing between U.S. government agencies (Distribution Statements B and C) or to limit dissemination based upon the Director's discretion (Distribution Statement F). Further exceptions for the use of another distribution statement shall be submitted to the JIEDDO Security Office, in writing, with justification.

FOR OFFICIAL USE ONLY

11. DISCLOSURE OF INTELLIGENCE/THREAT INFORMATION

Data or information relating to threat systems or other intelligence derived material must bear the security markings of that intelligence/threat material. All dissemination of intelligence / threat information is controlled by the Director, COIC. Intelligence/threat information may be reproduced, released to subcontractors, provided instructions, and procedures approved by the COIC Director. Intelligence/threat information may be reproduced, released to subcontractors, provided instructions, and procedures approved by the Senior Intelligence Officer (SIO) are followed. Questions regarding such releases shall be referred to the SIO.

12. LOSS, COMPROMISE, OR SUSPECTED COMPROMISE

Report the loss, compromise, or suspected compromise of classified JIEDDO information or material to the JIEDDO Security Office, 703-601-4744, within 24 hours of the incident.

13. COMPILATION OF INFORMATION.

In some circumstances, classification may be required if the compilation of unclassified items of information provide an inference that warrants classification. Similarly, a higher classification may be assigned to a compilation of information if the compilation provides an added factor that warrants higher classification than that of its component parts. Classification on this basis will be used sparingly, and complete justification of this classification method will be stated on the title or first page of the document. The classification and marking process is as follows:

- When a document comprises individually unclassified items of information is classified, by compilation, the overall classification shall be marked conspicuously at the top and bottom of each page and the outside front and back covers (if applicable). An explanation of the basis for classification by compilation shall be placed on the face of the document or included in the text.
- If portions, standing alone, are unclassified, but the document is classified by compilation or association, those portions shall be marked "U" and the document and pages shall be marked with the classification of the compilation. An explanation of the classification or the circumstances involved with association must be included.
- If individual portions are classified at one level and the compilation is a higher classification, each portion shall be marked with its own classification and the document and pages shall be marked with the classification of the compilation. An explanation of the classification by compilation is required.

FOR OFFICIAL USE ONLY

14. REASONS FOR CLASSIFYING

The reasons for classifying information in this SCG are in accordance with Part I, Section 1.4, Executive Order 12958 (as amended). They are:

- 1.4a – Military plans, weapons systems, or operations
- 1.4b – Foreign government information
- 1.4d – Foreign relations or foreign activities of the United States, including confidential sources; scientific, technological, or economic matters relating to national security
- 1.4 e – Scientific, technological, or economic matters
- 1.4 g – Vulnerabilities or capabilities of the system, installation, projects, or plans relating to the national security

15. DEFINITIONS

Classified Performance Capabilities or Limitations: Information that if disclosed would;

- 1) damage national security through facilitating adversary denial, degradation, disruption, deception, or destruction of mission essential or critical system(s), or
- 2) would require major modifications to an acquisition program or operational system to maintain the technological advantage of the system during its projected operational life time.

Compromise a Future Capability: Anything not in the inventory now and is planned to be developed; not a current capability. Applies to research, development and acquisition efforts.

Confidential: Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to national security that the original classification authority is able to identify or describe.

Critical Information: TBD by the supported organization. Different organizations may deem information differently as to its criticality. Determination and defense of information as critical is up to the supported organization.

Critical Program Information (CPI): Information, technologies, or systems that, unto themselves, if compromised would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction.

Effectiveness of Forces: TBD by supported organization. Usually refers to squad to division level. Different organizations may deem information differently as to its impact on the effectiveness of forces. For example; information that may impact the effectiveness of a Special Forces unit compared to a Battalion is potentially considerable. Determination and defense of information is up to the supported organization.

FOR OFFICIAL USE ONLY

Effectiveness of Major Forces: TBD by supported organization. Usually refers to theater level; unified command; combination of Military Departments (MILDEPS). Different organizations may deem information differently as to its impact on the effectiveness of major forces. Determination and defense of information is up to the supported organization.

Enhanced System Capability: An improvement over existing performance or capabilities found on similar systems.

Low- Level Intelligence Collection Capability: Focused on low- level counterintelligence, Human Intelligence (HUMINT) sources, e.g., bartender, "beat cop," or low- level detection capability, e.g., unattended ground sensors.

Mission Critical: A mission essential item whose disruption or destruction immediately degrades the ability of the force to command, control, or effectively conduct combat operations. For example, disruption or destruction of the mechanism used to fuse a system-of-systems (e.g., C4ISR) would result in the immediate inability for the separate system to act in concert as a system-of-systems.

Mission Essential: Those items required to support approved emergency and/or war plans, and where those items are used to:

- 1) destroy the enemy or the enemy's capacity to continue war;
- 2) provide battlefield protection of personnel;
- 3) communicate under war conditions;
- 4) detect, locate, or maintain surveillance over the enemy;
- 5) provide combat transportation and support of men and materiel; and/or
- 6) support training functions.

National Military Objectives: Protect the United States against external attacks and aggression; prevent conflict and surprise attack, and prevail against adversaries. These are the ends of the strategy and help to assure allies and friends, dissuade adversaries, and deter aggression and coercion while ensuring the armed forces remain ready to defeat adversaries should deterrence and dissuasion fail. They serve as benchmarks to assess levels of risk and help to define the types and amounts of military capabilities required.

National Objectives (for DoD): The aims derived from national goals and interests, toward which a national policy or strategy is directed and efforts and resources of the nation are applied.

National Security Strategy (for DoD): The art and science of developing, applying, and coordinating the instruments of national power (diplomatic, economic, military, and informational) to achieve objectives that contribute to national security. Also called national strategy or grand strategy.

FOR OFFICIAL USE ONLY

NOFORN: (NOT RELEASABLE TO FOREIGN NATIONALS) Under authority of Director of Central Intelligence, this marking is used for identified *classified intelligence* that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-US citizens without permission of the originator and in accordance with provisions of DCID 6/7 and NDP-1. Cannot be used with REL TO [country codes] or EYES ONLY on page markings (when a document contains both NOFORN and REL TO or NOFORN and EYES ONLY portions, NOFORN takes precedence for the markings at the top and bottom of the page).

Reveal a National Security Objective: Fact of statement that would reveal an undisclosed objective or intention—that is covert in nature. Details of how we plan to achieve national security objectives (primarily planning oriented).

Secret: Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Senior Leadership: President of the US (POTUS); Cabinet Members, Pentagon Senior Leadership, etc.

Sensitive Information: TBD by the supported organization. Different organizations may deem information differently as to its sensitivity. Determination and defense of information as sensitive is up to the supported organization.

Sensitive Intelligence Collection Capability: To be determined by the user or developer of that capability.

Significant Impairment: Any characteristic or concept, design or component that offers a technical disadvantage of enough magnitude to be potentially disruptive in an operational or advanced system.

State of the Art: The highest level of development, as of a device, technique, or scientific field, achieved at a particular time. For a system or technology that has no known baseline to determine its relative level of development, the very nature of it being the first of a kind, makes it state of the art.

Strategic Advantage: Operational superiority provided via military instruments that enables one nation or group of nations effectively to control the course of a military or political situation beyond a battle or engagement.

Strategic Disadvantage: Inverse of strategic advantage (see above definition).

FOR OFFICIAL USE ONLY

Tactical Advantage: Operational superiority provided via unit and system performance and capabilities during battles and engagements planned and executed to accomplish military objectives assigned to tactical units or task forces.

Tactical Disadvantage: Inverse of tactical advantage (see above definition).

Threaten the Country's Ability to Wage War: Identification of details of war plans that would reveal overall objectives or intentions.

Top Secret: Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security that the original classification authority is able to identify or describe.

Weaken the Country's Ability to Wage War: Identification of specific details of war plans in a theater of operation including use of tactical capabilities and mission essential items.

Significantly Weaken the Country's Ability to Wage War: Identification of specific dependencies and objectives in a theater of operation or sub area of a Unified Command to include strategic capabilities and mission critical items.

Threaten the International Position of the US: Damage US credibility with a foreign government.

Weaken the International Position of the US: Negative impact to the international position of the US and its ability to negotiate with foreign governments.

Significantly Weaken the International Position of the US: Inability of the US to successfully negotiate with a foreign government for a significant period of time.

Unique and Fragile Intelligence Collection Capability: To be determined by the user or developer of that capability.

FOR OFFICIAL USE ONLY

Only trained FDOs who have been issued a Delegation of Disclosure Authority Letter (DDL) can authorize the disclosure or release of classified military information to authorized representatives of foreign governments or international organizations as outlined in this guide.

ADMINISTRATION DATA

Element	Level	Duration	Remarks
JIEDDO Goal, Mission and Purpose			
JIEDDO mission	U		Public Release and Distribution Statement A applies for the following description: JIEDDO shall focus (lead, advocate, coordinate) all Department of Defense actions in support of Combatant Commanders and their respective Joint Task Forces' efforts to defeat improvised explosive devices as weapons of strategic influence. (DoDD 2000.1E)
JIEDDO organizational structure (Line and block chart identifying position only)	U		
JIEDDO organizational structure (Line and block chart identifying personnel by name)	U		Mark and handle as FOUO, FOIA exemption 2 applies.
JIEDDO Goals and Objectives	U		Mark and handle as FOUO, FOIA exemption 2 applies. Specific technological goals and objectives associated with real or postulated threats will be addressed by other portions of this SCG
JIEDDO Resources			
Financial plans	U		
Financial plans with classified program Names	U		Classify as directed by program security classification guide. FOIA 1(b)(2)(a).
JIEDDO budget	U		
Cost, pricing, or funding for individual systems, subsystems, or components	See Remarks		If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies. FOIA exemption 4 may apply to certain proprietary or trade secret information provided by vendors.

FOR OFFICIAL USE ONLY

			If individual project budget reveals a sensitive relationship between the JIEDDO and other DoD organizations, US government organizations, or a foreign government or foreign owned company then classify in accordance with the guidance provided by the other organization, government, or the contractor relationship portion of this document.
Budget levels for projects	See Remarks		If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies. If individual project budget reveals a sensitive relationship between the JIEDDO and other DoD organizations, US government organizations, or a foreign government or foreign owned company then classify in accordance with the guidance provided by the other organization, government, or the contractor relationship portion of this document..
Production quantities and delivery rates	U		If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies.
Manpower, overall by year, category, skill, and system	U		
Manpower, overall by year, category, skill, system, and individual name	U	If classified, declass in accordance with proponent SCG.	Mark and handle as FOUO, FOIA exemption 2 applies.
Identification of a particular installation, facility or range associated with the JIEDDO	U-S		Classify as directed by program security classification guide.
Aggregate number of C-IED systems deployed in a particular theater of operation or to a particular unit	See Remarks		Peacetime Situations: Derivative according to documents such as Table or Organization and Equipment. Combat Situations: Derivative according to operational SCG such as MNF-I or OEF SCG.
JIEDDO Schedules			
Organization master schedule	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Specific program/project status	U-S		Mark and handle as FOUO, FOIA exemption 2 applies.
Development milestones	U-S		Mark and handle as FOUO, FOIA exemption 2 applies.

FOR OFFICIAL USE ONLY

Procurement milestones	U-S		Mark and handle as FOUO, FOIA exemption 2 applies.
Contractor Relations			
Partial or full list of contractors producing or procuring IED defeat systems or component pieces	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Data on parts, accessories and equipment available in the open market or produces for commercial use not tied or related to IED defeat capabilities	U		Public release and distributions statement A applies.
DD 254s	U - S	Declassify 10 years from date of creation	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.
Statements of work	U - S	Declassify 10 years from date of creation	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies.
Organization Security			
Results of program protection risk management processes / analysis	See Remarks		Mark and handle as FOUO, FOIA exemption 2, 5 applies. Specific information may be derivatively classified from documents such as threat assessments, etc.
Details of specific protection measures associated with the JIEDDO Note: Specific protection measures are those relative to the JIEDDO and not generalized guidance	See Remarks (U-S)		Mark and handle as FOUO, FOIA exemption 2 applies. <u>RAM Measures at a minimum is SECRET</u> Specific information may be derivatively classified from documents such as threat assessments, etc.

FOR OFFICIAL USE ONLY

JIEDDO OPERATIONS

Element	Level	Duration	Remarks
General information regarding the requirements for the JIEDDO and IED defeat systems	See Remarks	Declassify 10 years from date of creation	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Specific technical requirements associated with a specific system, subsystem or component	U-S	Declassify 10 years from date of creation	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Identification of key performance threshold/objective parameters associated with the JIEDDO and specific IED defeat system, subsystem or component	See Remarks	Declassify 10 years from date of this document	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Operational capabilities/shortfalls	See Remarks (U-TS)	Declassify 10 years from date of this document	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 and/or 5 applies.
IED- Related SIGACTS	See Remarks (U-TS)		Classify in accordance with SCG for the program or system. All theater derived SIGACTS are SECRET.
JIEDDO specific tactic's techniques and procedures (TTPs)	See Remarks (C-TS)	Declassify 10 years from date of this document	Classify in accordance with the SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 and/or 5 applies.
JIEDDO CONOPS	U-S	Declassify 10 years from date of this document	Classify in accordance with SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 and/or 5 applies.
Movement of JIEDDO related personnel and equipment.	See Remarks		If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.) If

Formatted: Font: Bold

FOR OFFICIAL USE ONLY

			UNCLASSIFIED FOIA 2 potentially applies.
Field team locations	See Remarks		If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.).
Field Team Composition, disposition, and strengths	See Remarks	Declassify 10 years from date of this document	If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.). If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2.
Field Team requirements and mission	See Remarks	Declassify 10 years from date of this document	If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.). Specific information not covered in an operational classification guide; classify in accordance with the SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2.
Analysis products by JIEDDO intelligence analysts	See Remarks		Classify in accordance with the applicable Intelligence Community classification guide. If no guidance is available refer to DoDD 5240.08 (DOD CI SCG, December 2005, if UNCLASSIFIED FOIA 2, 4 and 5 applies).
JIEDDO intelligence requirements	S	Declassify 10 years from date of this document	Classify in accordance with current markings or the SCG for the operation, program or system, (if UNCLASSIFIED FOIA 2, 4 and 5 applies).
Specific IED- related system employment locations	See Remarks	Declassify 10 years from date of this document	If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.) (if UNCLASSIFIED FOIA 2, 4 and 5 applies).
Specific IED- related system employment methods	See Remarks	Declassify 10 years from date of this document	If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.). Specific information not covered in an operational or system specific classification; classify in accordance with the SCG for the program or system. Classification of employment locations may be classified a higher levels or within compartmented channels based upon operational guidance.

FOR OFFICIAL USE ONLY

			If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 and 5 potentially applies.
IED lessons learned	U-S	Declassify 10 years from date of this document	<p>If resulting from combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.).</p> <p>For JIEDDO specific developed lessons learned treat as:</p> <p>Classify in accordance with current classification or the SCG for the program or system.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 and/or 5 applies.</p>
Initial Review Group (IRG) internal decision- making processes and results	U-S	Declassify 10 years from date of this document	<p>Classify in accordance with current markings or the SCG for the operation, program or system.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
Technology Review Group (TRG) internal decision- making processes and results	U-S	Declassify 10 years from date of this document	<p>Classify in accordance with current markings or the SCG for the operation, program or system.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
JIEDD Requirements, Resources and Acquisition Board (JR2AB) internal decision making processes and results	U-S	Declassify 10 years from date of this document	<p>Classify in accordance with current markings or the SCG for the operation, program or system.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
Joint Integrated Product Team internal decision- making processes and results	U-S	Declassify 10 years from date of this document	<p>Classify in accordance with current markings or the SCG for the operation, program or system.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>

C-JED Operational/Intelligence Integration Center (COIC)

For Further Information Refer to Annex A of this Classification Guidance

FOR OFFICIAL USE ONLY

COIC mission	U		
--------------	---	--	--

RED AND BLUE TEAM ACTIONS

Element	Level	Duration	Remarks
Fact that JIEDDO performs red teaming and blue teaming	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Red team and blue team reports	See Remarks		Results are to be classified at the same level as the items or systems being Red Teamed or Blue Teamed – classify in accordance with information revealed. If system specific classification guidance exists, then classify in accordance with that guidance. Specific Information not covered in a component classification guide is treated as derivative from other sections of this SCG. Classification of red team and blue team plans and results is dependent on the security classification of the information involved.
Field team prototypes of possible new threat modes or techniques	See Remarks		Prototypes without accompanying explanatory information will be handled as FOUO. FOIA 4 potentially applies. When associated with specific Red Team and Blue Team reports classify at the same level as the associated report.
Limitations or vulnerabilities associated with IED defeat systems or subsystems revealed by Red Teaming or technical gaming	See Remarks	Declassify 10 years from date of this document	Classify according to the level of information revealed through the association of limitations or vulnerabilities of specific IED defeat systems. If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as: CONFIDENTIAL if loss of information would reveal or

FOR OFFICIAL USE ONLY

			<p>compromise a future capability.</p> <p>SECRET if details would lead to loss of research, development and engineering; scientific, or technical information that would lead to a tactical disadvantage.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.</p>
--	--	--	---

JIEDDO SYSTEM AND SUBSYSTEM PERFORMANCE AND CAPABILITIES

This section applies to all IED detection and defeat systems and subsystems.

(Many such systems fall under a different Original Classification Authority than JIEDDO owned information – i.e. Warlock Red falls under the authority of PM SW and PEO IEW&S and therefore all classification determinations for this system are found in the Joint counter radio controlled improvised explosive service electronic warfare Program Security Classification Guide) (CREW)

Element	Level	Duration	Remarks
General information regarding the capabilities of IED defeat systems or subsystems	U		General information is that which can be found in unclassified requests for proposals and approved JIEDDO press releases and media guidance, and documents marked with FOIA distribution statement A.
Specific details regarding the capabilities of IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	<p>If system specific classification guidance exists, then classify in accordance with that guidance.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 or 5 applies.</p>
Emerging IED defeat capabilities or systems	See Remarks	Declassify 10 years from date of this document	<p>If system specific classification guidance exists, then classify in accordance with that guidance.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
(CREW) System or Subsystem	See Remarks		<p>For guidance on all CREW system, refer to the Joint Counter Radio Controlled Improvised Explosive Service Electronic Warfare Program Security Classification Guide, 8 August, 2006 (OPNAVINST 5513.8B-88).</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.</p>
Maximum range of detection / defeat for	See Remarks	Declassify 10 years	If system specific classification guidance exists, then classify

FOR OFFICIAL USE ONLY

IED defeat system or subsystem		from date of this document	in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Detection rates	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
The fact that specific IED defeat systems will be used to protect specifically named VIP's	See Remarks (S-TS)	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. The general statement that C-IED systems are used for VIP protection is UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 and/or 5 applies. The fact C-IED systems are being used to protect specific VIPs is classified SECRET based on the program SCG, the loss of information could lead to a tactical disadvantage. Classification of C-IED systems being used to protect specific VIPs may be classified at higher levels or within compartmented channels based upon operational guidance.
Effectiveness of IED defeat systems or subsystems against general threats	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. General categories of threats that C-IED systems are designed to counter (e.g. car alarms, cell phones, etc) UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Effectiveness of IED defeat systems or subsystems against specific threats	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Specific system Concept of Operations (CONOPS)	See Remarks (C-S)	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA

FOR OFFICIAL USE ONLY

			exemption 2, 4 or 5 applies.
Specific system tactics, techniques, procedures (TTPs)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Frequency ranges when expressed in general terms (such as Band A / Band B)	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Frequency bands expressed in general terms that do not reveal actual operating parameters is UNCLASSIFIED.
Frequency bands associated with specific IED defeat systems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. Listing of actual operating frequencies, frequency bands, or entire spectrum coverage is SECRET – the loss of information could lead to a tactical disadvantage. If UNCLASSIFIED, FOIA 4 potentially applies.
Antennas associated with IED defeat systems or subsystems	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. The fact that specific antennas are being used for C-IED systems is UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies. If performance characteristics of an antenna are classified, then classify in accordance with the applicable SCG.
IED defeat system or subsystem reliability, maintainability, and supportability	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Technical details of signal processing or jamming techniques / parameters	See Remarks	Declassify 10 years from date of this	If system specific classification guidance exists, then classify in accordance with that guidance.

FOR OFFICIAL USE ONLY

		document	If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Threat characteristics that are used to determine which IED defeat system or subsystem to employ	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
RF Output power or other information that would reveal effective range of operation	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Input sensitivity or other information that would reveal system or subsystem detection range	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Interoperability between various IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Interoperability between IED defeat systems or subsystems and other equipment (communication equipment, weapons systems, etc)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.

FOR OFFICIAL USE ONLY

JIEDDO RELATED HARDWARE / SOFTWARE

(Some Hardware and Software falls under a different Original Classification Authority than JIEDDO owned information – i.e. Warlock Red falls under the authority of PM SW and PEO IEW&S and therefore all classification determinations for this system are found in the Joint Counter Radio Controlled Improvised Explosive Service Electronic Warfare Program Security Classification Guide)

Element	Level	Duration	Remarks
Technology Integration			
General description of technologies being considered for use by JIEDDO Note: Technologies that have actually been selected for use by JIEDDO are covered in the respective SCG	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as: UNCLASSIFIED - Mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Specific technical details of technologies being considered for use by JIEDDO Note: Technologies that have actually been selected for use by JIEDDO are covered in the respective SCG	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Design Details			
General information regarding IED defeat systems or components of systems	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Design specifications of IED defeat systems or components of systems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Specific technical details regarding IED defeat systems or components of systems (antennas, etc)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance.

FOR OFFICIAL USE ONLY

			If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Network architecture system view	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Network architecture technical view	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Network architecture network functions	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Software architecture	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Software source code	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Information assurance technical details (To include Cross Domain Guard, Network Intrusion Detection System, Key Fill Bus, firewall, and switches)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Cryptographic capabilities and equipment	See Remarks		Contact OPR COMSEC material and controlled cryptographic items shall be handled, marked and safeguarded in accordance with policies and procedures of the National Security Agency. If UNCLASSIFIED, mark and handle as FOUO, FOIA

FOR OFFICIAL USE ONLY

			exemption 2, 4 or 5 applies.
Modeling and Simulation			
Fact that modeling and simulation is used for design and validation of a specific system, subsystem or component	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as UNCLASSIFIED - Mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Operational parameters for specific modeling and simulation at the force, system, subsystem or component level	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Details of specific items in the modeling and simulation database	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Results of the modeling and simulations	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Commercial Off the Shelf (COTS) / Government Furnished Equipment (GFE)			
Fact that the JIEDDO uses COTS/GFE systems	U		Public Release and Distributions Statement A applies.
Association of COTS/GFE used on a particular IED defeat system, subsystem, or component	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Mark and handle as FOUO, FOIA exemption 4 potentially applies.
Modification of COTS/GFE	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Unusual or unique application of GFE	See Remarks	Declassify 10 years	If system specific classification guidance exists, then classify

FOR OFFICIAL USE ONLY

		from date of this document	in accordance with that guidance If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Technical details about modification of COTS/GFE	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Manufacturing / Fabrications			
Fact that unique / non-traditional manufacturing processes are used to develop IED defeat systems, subsystems, or components	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Technical details of unique / non-traditional manufacturing processes used to develop IED defeat systems, subsystems, or components	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Integration			
Fact that unique / non-traditional integration processes are used to develop IED defeat systems, subsystems, or components	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Identification of unique / non-traditional integration techniques with specific IED defeat systems, subsystems, or components	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Technical details of unique / non-traditional integration techniques relative to IED defeat systems, subsystems, or components	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 3, 4 and 5 applies.
External / Internal Views			
External view of IED defeat systems, subsystems, or components (including	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance

FOR OFFICIAL USE ONLY

drawings, photographs, etc.)			If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4.
Internal view of IED defeat systems, subsystems, or components (including technical drawings of systems, components such as wiring plans, blueprints, and section cutaways)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Anti-Tamper			
General information regarding the fact that anti-tamper is used on IED defeat systems, subsystems, or components	U		
Technical details regarding implementation of anti-tamper to deter / delay attempts at reverse engineering of hardware / software of IED defeat systems, subsystems, or components	See Remarks		Refer to the Anti Tamper SCG, dated 1 March 2001. If UNCLASSIFIED, FOIA exemption 2, 4 or 5 potentially applies.

VULNERABILITIES AND WEAKNESSES

Element	Level	Duration	Remarks
General information regarding vulnerabilities and limitation of IED defeat systems or subsystems (i.e. information found via open sources related to common vulnerabilities such as the statement that "coalition troops are vulnerable to VBIED attacks")	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. <u>Combination of open source material may classify information</u> General information not covered in a component classification guide is treated as: UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Details of specific operational limitations and vulnerabilities of IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.
Identification of system susceptibilities in the presence of a validated threat to a specific IED defeat system or subsystem	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance.

FOR OFFICIAL USE ONLY

			If UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.
Technical details of specific countermeasure employed (e.g. ECM, Anti-Tamper, Signature Management, etc)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, FOIA, exemption 4 or 5 potentially applies.
Effectiveness of specific countermeasures	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If, UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.
Information regarding signals or initiation means which may not be detected or which may be immune to specific IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If, UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.

INDUSTRY TEST AND EVALUATIONS

Element	Level	Duration	Remarks
Details of IED defeat system or subsystem test plan	See Remarks		Testing is to be classified at the same level as the item being tested – classify in accordance with information revealed. If system specific classification guidance exists, then classify in accordance with that guidance. If, UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.
Identification of specific dates for IED defeat systems or subsystem tests	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Identification of specific test locations associated with IED defeat systems or	U		Mark and handle as FOUO, FOIA exemption 2 applies.

FOR OFFICIAL USE ONLY

subsystems			
Identification of specific or specialized test instrumentation or equipment associated with IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	<p>Classify according to the level of information revealed through the association of specialized test equipment with specific IED Defeat systems.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.</p>
Predicted test data	See Remarks		<p>Testing is to be classified at the same level as the item being tested – classify in accordance with information revealed.</p> <p>Predicted test data that provides specific performance and capability data on IED defeat System or Subsystem shall be classified in accordance with that component Security Classification Guide.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.</p>
Raw test data	See Remarks		<p>Testing is classified at the same level as the item being tested – classify in accordance with information revealed.</p> <p>Raw data that provides specific performance and capability data on IED defeat System or Subsystem shall be classified in accordance with that components Security Classification Guide.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.</p>
Reduced test data	See Remarks		<p>Testing is classified at the same level as the item being tested – classify in accordance with information revealed.</p> <p>Reduced test data that provides specific performance and capability data on IED defeat System or Subsystem components shall be classified in accordance with that components Security Classification Guide.</p> <p>If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.</p>

FOR OFFICIAL USE ONLY

TRAINING

Element	Level	Duration	Remarks
Training location specific to the JIEDDO and IED defeat systems, subsystems, or components	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Training that reveals specific system information (e.g. design, development, capabilities, vulnerabilities, etc.) Note: This element includes live training, virtual training, and constructive training.	See Remarks	Declassify 10 years from date of this document	Classify in accordance with the level of information revealed during the training. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Training Aids (Includes both IED training devices and C-IED training devices)	U		If, UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.

MAINTENANCE

Element	Level	Duration	Remarks
Location of specialized maintenance organizations associated with the JIEDDO and IED defeat systems, subsystems, or components	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.
Association of maintenance equipment or tools that may reveal specific system information	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies.
Maintenance that reveals specific system information (e.g. design, development, capabilities, vulnerabilities, etc.)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance.

FOR OFFICIAL USE ONLY

			If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies.
Field level maintenance	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.
Intermediate level maintenance	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.
Depot level maintenance	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.

INSTRUCTIONS FOR PREPARING AND ARRANGING RECORD OF TRIAL

USE OF FORM - Use this form and MCM, 1984, Appendix 14, will be used by the trial counsel and the reporter as a guide to the preparation of the record of trial in general and special court-martial cases in which a verbatim record is prepared. Air Force uses this form and departmental instructions as a guide to the preparation of the record of trial in general and special court-martial cases in which a summarized record is authorized.

Army and Navy use DD Form 491 for records of trial in general and special court-martial cases in which a summarized record is authorized. Inapplicable words of the printed text will be deleted.

COPIES - See MCM, 1984, RCM 1103(g). The convening authority may direct the preparation of additional copies.

ARRANGEMENT - When forwarded to the appropriate Judge Advocate General or for judge advocate review pursuant to Article 64(a), the record will be arranged and bound with allied papers in the sequence indicated below. Trial counsel is responsible for arranging the record as indicated, except that items 6, 7, and 15e will be inserted by the convening or reviewing authority, as appropriate, and items 10 and 14 will be inserted by either trial counsel or the convening or reviewing authority, whichever has custody of them.

1. Front cover and inside front cover (chronology sheet) of DD Form 490.
2. Judge advocate's review pursuant to Article 64(a), if any.
3. Request of accused for appellate defense counsel, or waiver/withdrawal of appellate rights, if applicable.
4. Briefs of counsel submitted after trial, if any (Article 38(c)).
5. DD Form 494, "Court-Martial Data Sheet."
6. Court-martial orders promulgating the result of trial as to each accused, in 10 copies when the record is verbatim and in 4 copies when it is summarized.
7. When required, signed recommendation of staff judge advocate or legal officer, in duplicate, together with all clemency papers, including clemency recommendations by court members.

8. Matters submitted by the accused pursuant to Article 60 (MCM, 1984, RCM 1105).

9. DD Form 458, "Charge Sheet" (unless included at the point of arraignment in the record).

10. Congressional inquiries and replies, if any.

11. DD Form 457, "Investigating Officer's Report," pursuant to Article 32, if such investigation was conducted, followed by any other papers which accompanied the charges when referred for trial, unless included in the record of trial proper.

12. Advice of staff judge advocate or legal officer, when prepared pursuant to Article 34 or otherwise.

13. Requests by counsel and action of the convening authority taken thereon (e.g., requests concerning delay, witnesses and depositions).

14. Records of former trials.

15. Record of trial in the following order:

- a. Errata sheet, if any.
- b. Index sheet with reverse side containing receipt of accused or defense counsel for copy of record or certificate in lieu of receipt.
- c. Record of proceedings in court, including Article 39(a) sessions, if any.
- d. Authentication sheet, followed by certificate of correction, if any.
- e. Action of convening authority and, if appropriate, action of officer exercising general court-martial jurisdiction.
- f. Exhibits admitted in evidence.
- g. Exhibits not received in evidence. The page of the record of trial where each exhibit was offered and rejected will be noted on the front of each exhibit.
- h. Appellate exhibits, such as proposed instructions, written offers of proof or preliminary evidence (real or documentary), and briefs of counsel submitted at trial.